INDIANA STATE POLICE

Indiana Intelligence Fusion Center

Face Recognition Policy

June 1, 2022

The Indiana Intelligence Fusion Center Face Recognition Policy represents the privacy policy applicable to all IIFC operations and activities.

Table of Contents

{Page intentionally left blank}

Indiana Intelligence Fusion Center (IIFC) Face Recognition Policy

Purpose Statement

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of deceased persons, or persons unable to identify themselves. The **Indiana Intelligence Fusion Center** has implemented a face recognition program to support the investigative efforts of law enforcement and public safety agencies both within and outside the State of Indiana.

It is the purpose of this policy to provide Indiana Intelligence Fusion Center personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a face recognition (FR) program. This policy will ensure that all FR uses are consistent with authorized purposes.

The purpose of this privacy, civil rights, and civil liberties (P/CRCL) protection policy is to promote IIFC and user conduct that complies with applicable federal and state law and assists the center and its users in:

- Increasing public safety and improving national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health.
- Minimizing the threat and risk of damage to real or personal property.
- Protecting individual privacy, civil rights, civil liberties, and other protected interests.
- Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the reluctance of individuals or groups to use or cooperate with the justice system.
- Supporting the role of the justice system in society.
- Promoting governmental legitimacy and accountability.
- Not unduly burdening the ongoing business of the justice system.
- Making the most effective use of public resources allocated to public safety agencies.
-

All deployments of the face recognition program are for official law enforcement sensitive (LES). The provisions of this policy are provided to support the following authorized uses of face recognition information:

- Reasonable suspicion exists that the subject of the criminal intelligence information is involved with or has knowledge of possible criminal or terrorist activity; and
- The criminal intelligence information is relevant to the criminal or terrorist activity.
- Indiana Intelligence Fusion Center Privacy Policy.

Policy Applicability and Legal Compliance

The policy is applicable to all personnel working in direct support of the IIFC.

This policy was established to ensure that all images are lawfully obtained, including face recognition probe images obtained or received, accessed, used, disseminated, retained, and purged by the Indiana Intelligence Fusion Center. This policy applies to:

- Images contained in a known identity face image repository and its related identifying information.
- The face image searching process.
- Any results from face recognition searches that may be accessed, searched, used, evaluated, retained, disseminated, and purged by the IIFC.
- Lawfully obtained probe images of unknown suspects will not be maintained.

An outside agency, or investigators from an outside agency, may request face recognition searches to assist with investigations only if:

- o The outside agency is a law enforcement agency or provides a law enforcement function that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in the IIFC Privacy Policy and/or Indiana State law. The requestor shall provide their contact information (requestor's name, requestor's agency, address, and phone number), and lawful reason for request.

The IIFC shall provide the following statement to any identification provided to the requestor: o *The result of a face recognition search is provided by the Indiana Intelligence Fusion Center only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.*

Governance and Oversight

Primary responsibility for the operation of the IIFC, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis destruction, sharing, or disclosure of information; and the enforcement of this policy is assigned to the Executive Director of the IIFC.

The Indiana Intelligence Fusion Center Executive Director will be responsible for the following**:**

- Overseeing and administering the face recognition program to ensure compliance with applicable laws, regulations, standards, and policy.

The Indiana Intelligence Fusion Center face recognition program was established on January 1, 2018 in conjunction with the Indiana State Police. Personnel from the following agencies are authorized to request face recognition searches:

- Any Federal, State, Local, Tribal or governmental agency acting in a law enforcement capacity and making a lawful request or providing a lawfully obtained image for face recognition analysis under the guidelines of the IIFC Privacy Policy of this document.

IIFC privacy compliance is guided by a trained Privacy Officer who is appointed by the Executive Director. Violations of the privacy policy can be reported to the Executive Director, Assistant Director or to the Privacy Officer. Reporting can be made pursuant to the IIFC privacy policy.

Information

The Indiana intelligence fusion center may collect criminal intelligence information only if:

- Reasonable suspicion exists that the subject of the criminal intelligence information is involved with or has knowledge of possible criminal or terrorist activity; and
- The criminal intelligence information is relevant to the criminal or terrorist activity.

IIFC personnel are required to adhere to the ISE- SAR Functional Standard and state and federal laws for the receipt, collection, assessment, storage, access, dissemination, retention, and security of Suspicious activity reporting (SAR) information.

The IIFC may retain information that based on a level of suspicion of reasonably indicative behavior of pre-operational planning associated with terrorism," such as tips and leads or suspicious activity report (SAR) information, as it pertains to terrorist or criminal activity, subject to the policies and procedures specified in this policy.

- The ISE-SAR Functional Standard *does not alter law enforcement officers' constitutional obligations when interacting with the public*. This means, for example, that constitutional protections and agency policies and procedures that apply to a law enforcement officer's authority to stop, stop and frisk ("Terry Stop"), request identification, or detain and question an individual apply in the same measure to observed behavior *that is reasonably indicative of pre-operational planning associated with terrorism*. It is also important to recognize that many terrorism-related activities are now being funded via local or regional criminal organizations whose direct association with terrorism *may be tenuous*. This places law enforcement and homeland security professionals in the unique, yet demanding, position of identifying suspicious behaviors *as a by-product or secondary element in a criminal enforcement or investigative activity*.

The IIFC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as constitutional rights, including personal privacy and other civil liberties, and civil rights.

The IIFC will not seek or retain, and information-originating agencies will agree not to submit, information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

- When participating on a federal law enforcement task force or when documenting a SAR or an ISE-SAR in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion. However, those attributes may be documented in specific suspect descriptions for identification purposes.

The IIFC applies labels to agency-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

- the information pertains to all individuals pursuant to IC 10-11-9-4, and
- The information is subject to Federal and Indiana state laws restricting access, use, or disclosure, including, but not limited to, 18 USC 2721, IC 35-38-9 et seq., IC 31-39-8 et seq., IC 4-1-10 et seq., IC 5-2 et seq., IC 5-14-3 et seq., and 28 CFR, Part 23.

IIFC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency will assign categories to the information) to reflect the assessment, such as:

- Whether the information consists of tips and leads data, suspicious activity reports, criminal history or intelligence information, case records, conditions of supervision, or case progress, etc.;
- The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector);
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown); and;

- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

At the time a decision is made to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

- Not interfere with or compromise pending criminal investigations;
- Protect an individual's right of privacy, civil rights, and civil liberties; and
- There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

The IIFC will identify and review information that is originated by the IIFC prior to sharing that information in the ISE.

Acquiring and Receiving Face Recognition Information

The Indiana Intelligence Fusion Center (IIFC) is authorized to access and perform face recognition searches utilizing the following external repositories:

- Mug-shot images via the Indiana State Police Criminal Justice Data Division
- Vigilant Solutions general image file
- Images known to the IIFC and Law Enforcement of persons who are involved in criminal or terrorist activity.
- Images not owned by IIFC, but authorized access by MOU
- Open source images

For the purpose of performing face recognition searches, the IIFC and authorized IIFC personnel will obtain probe images or accept probe images from law enforcement or participating agencies only for the authorized uses identified in the IIFC Privacy Policy.
Information gathering (acquisition and access) and investigative techniques used by the IIFC and information-originating agencies are in compliance with and will adhere to applicable regulations and guidelines, including:

- 28 CFR, Part 23 regarding criminal intelligence information
- DHS' Fair Information Practice Principles (under certain circumstances, there may be exceptions to the Fair Information Practice Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal laws; or agency/center policy)
- Applicable constitutional provisions in, IC 10-11-9 et seq.

Information gathering techniques used by the IIFC will (and for originating agencies should) be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

External agencies that access and share information with the IIFC are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws.

The IIFC will make every effort to contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable federal, state, local, tribal, and territorial laws, statutes, and regulations and that these methods are not based on misleading information collection practices.

The IIFC will not directly or indirectly receive, seek, accept, or retain information from an individual or information provider that is legally prohibited from obtaining or disclosing the information.

The IIFC's SAR process provides for human review and vetting to ensure that information is both gathered in an authorized and lawful manner and, when applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating agency staff members will be trained to recognize those behaviors and incidents that are indicative of criminal activity associated with terrorism.

The IIFC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, ethnicity, national origin, religion, etc.) and civil liberties (speech, assembly, association, religious

Use of Face Recognition Information

The IIFC does not connect the face recognition system to any interface that performs live video surveillance, including surveillance cameras, drone footage, and body-worn cameras.

The following describes the Indiana Intelligence Fusion Center's (IIFC) manual face recognition search procedure, which is conducted in accordance with the IIFC Privacy Policy and this policy.

- Federal, State, Local, and tribal law enforcement personnel can submit a probe image of a subject with reasonable suspicion of involvement in crime or terrorism.
- Trained IIFC analysts will initially run probe images without filters, using a filtered search as a secondary search, if needed. In some cases, enhancements may be considered after running an image as is against the image repository in accordance with best established practices (See Appendix B). All enhancements and queries will be documented for audit purposes in accordance with bet established practices (See Appendix C).
- In the automated search, most likely candidates are returned to the analyst to analyze for confidence. The resulting candidates, if any, are then manually compared with the probe images and examined by an analyst. Analysts shall conduct the comparison of images, biometric identifiers, and biometric information in accordance with their training set by best established practices (see Appendix D).
  - If no likely candidates are found, the requesting entity will be informed of the negative results. In the case of a negative result, the images examined by the analyst will not be provided to the requesting entity.
- Analysts should submit the original probe images and subsequent examination results for a peer review of the probe and candidate images for verification by other analysts.
- The analyst will conduct an initial background investigation on potential matches, comparing information to known criminal case details before disseminating potential leads to originating agency.
- All entities receiving the results of a face recognition search, must be cautioned that the resulting candidate images do not provide positive identification of any subject, are considered advisory in nature as an investigative lead only, and do not establish probable cause, without further investigation, to obtain an arrest warrant without further investigation as well as any analyst obtained background information for each potential lead.

Sharing and Disseminating Face Recognition Information

The Indiana Intelligence Fusion Centers (IIFC) face recognition search information will not be:

- Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by the IIFC's agreement with the commercial vendor.
- Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, the IIFC and the originating agency may agree in writing in advance that the IIFC will disclose face recognition search information as part of its normal operations, including disclosure to an external auditor of the face recognition search information.
- Disclosed on a discretionary basis unless the originating agency has provided prior written approval or unless such disclosure is otherwise authorized by the MOU or agreement between the IIFC and the originating agency.
- Disclosed to unauthorized individuals or for unauthorized purposes.

Data Quality Assurance

- Original probe images will not be altered, changed, or modified in order to protect the integrity of the image. Any enhancements made to a probe image will be made on a copy, saved as a separate image, and documented to indicate what enhancements were made, including the date and time of change.
- IIFC analysts will analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a face recognition search.
- The IIFC considers the results, if any, of a face recognition search to be advisory in nature as an investigative lead only. Face recognition search results are **not** considered positive identification of a subject and do not, on their own, establish probable cause, without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

The IIFC will make every reasonable effort to perform routine maintenance, upgrades and enhancements, testing, and refreshes of the face recognition system to ensure proper performance, including the following:

- Personnel shall assess the face recognition system on a regular basis to ensure performance and accuracy.
- Malfunctions or deficiencies of the system will be reported to the Director of Operations upon discovery of the malfunctions or deficiencies.

The integrity of information depends on quality control and correction of recognized errors which is key to mitigating the potential risk of misidentification or inclusion of individuals in a possible identification. The IIFC will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face recognition information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The IIFC will correct the information or advise the process for obtaining correction of the information.

Disclosure Requests

Face recognition information will only be disclosed to the public in accordance with IIFC's privacy policy.

Security and Maintenance

- The IIFC will comply with generally accepted industry or other applicable standards for security, in accordance with Indiana Office of Technology to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related IIFC activity.
- All entities to the project will operate in a secure environment protected with multiple layers of security from external intrusion and will utilize secure internal and external security and privacy safeguards against network intrusions, such as strong multifactor authentication; encrypted communications; firewalls; and other reasonable physical technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system. Any access to IIFC face recognition information from outside the facility will be allowed only over secure networks.
- All results produced by the IIFC as a result of a face recognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee.
- All face recognition equipment, face recognition software, algorithm, thresholds, and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates and adjustments as appropriate.
- The IIFC and contributing entities will store face recognition information in a manner that ensures it cannot be modified, accessed, or purged except by personnel authorized to take such actions.
- Authorized access to the IIFC face recognition system will be granted only to personnel whose positions and job duties require such access.

- Usernames and passwords to the face recognition system are not transferrable, must not be shared by IIFC personnel, and must be kept confidential.
- Queries made to the IIFC's face recognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.
- The IIFC will maintain an audit trail of requested, accessed, searched, or disseminated IIFC held face recognition information, via Vigilant Solutions. An audit trail will be kept for requests, access, and searches of face recognition information for specific purposes and of what face recognition information is disseminated to each individual in response to the request.

Information Retention and Destruction

- All images utilized by the IIFC, via the Indiana State Police Criminal Justice Data Division, will be stored for a period determined by the Indiana State Police Criminal Justice Data Division, the Indiana Intelligence Fusion Center Privacy Policy, State and Federal law, and this policy.
- Once a face recognition image is downloaded by IIFC personnel and incorporated into a criminal intelligence record or an investigative case file, the face recognition information is then considered criminal intelligence or investigative information, and the laws, regulations, and policies applicable to that type of information or criminal intelligence govern its use.
- Any images that do not originate with the IIFC will remain in the custody and control of the originating agency and will not otherwise be transferred to any other entity without authorization from the originating agency. Images provided by an agency will be considered lead information and retained per the IIFC privacy policy pertaining to lead information, until such time that the originating agency provides an update to IIFC.
- The IIFC retains the right to remove images from the repository earlier than the retention period, based on the limitations of information storage requirements and subject to any applicable record retention laws and statutory disclosure mandates. Early removal, however, will not be used as a means for intentionally interfering with a lawful complaint or a public records request. The retention period may be modified at any time by the IIFC subject to applicable legal requirements.
- Any persons confirmed to be innocent will be purged from the system immediately upon notification.
- Probe images are stored in an analyst working file for only as long as needed to analyze the request. Probe images will not be retained beyond privacy policy guidelines. No other images will be retained by IIFC. All images and results will be provided to the originating agency for their retention.
- Face recognition search results may be saved within the entity's system audit log for audit purposes only. The audit log is available only to the Executive Director, Assistant Director, Director of Operations and Director of Intelligence and Analysis. Face recognition searches cannot be performed using the audit log.

Accountability and Enforcement

- The IIFC will follow procedures and practices by which it can ensure and evaluate the compliance of users with the face recognition system requirements and with the provisions of this policy and applicable law. This will include logging access to face recognition information, may include any type of medium or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related activity, and will entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least annually, and a record

  of the audits will be maintained by the Privacy Officer, of the IIFC pursuant to the retention policy. Audits may be completed by an independent third party or a designated representative of the IIFC
- The Assistant Director**,** will review and update the provisions contained in this face recognition policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the face recognition system; the audit review; and public expectations.

Enforcement

If IIFC personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, the Executive Director of the IIFC will:

- Suspend or discontinue access to information by the IIFC entity personnel, the participating agency, or the authorized user.
- Apply appropriate disciplinary or administrative actions or sanctions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

{Remainder of page Intentionally left blank)

Appendix A—Glossary of Terms and Definitions

The following is a list of terms and definitions used within the policy or provided for the purpose of enhancing the reader's understanding of the topics discussed.

Access—Information access is being able to get to particular information on a computer (usually requiring permission to use). Web access means having a connection to the internet through an access provider or an online service provider.

Access Control—The mechanisms for limiting access to certain information, based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role- or user-based.

Acquisition—The means by which an entity obtains face recognition information through the exercise of its authorities.

Agency—See Participating Agency.

Algorithm—An algorithm is a procedure or formula for solving a problem, based on conducting a sequence of specified actions. A computer program can be viewed as an elaborate algorithm. Algorithms can perform calculation, data processing, and automated reasoning tasks and are widely used throughout all areas of information technology.

Analysis—Refer to Image Analysis.

Attributes—Physical characteristics, such as gender, race, age, hair color, etc. that can be applied to a face recognition search.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail, such as what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security and used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provides a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

Authorization—The process of granting a person, a computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, a computer process, or a device requesting access that is verified through authentication. See Authentication.

Automated Face Recognition (AFR)—Automated face recognition (AFR) software compares patterns within the field of computer vision. Such approaches do not rely upon intrinsic models of what a face is, how it should appear, or what it may represent. In other words, the matching is not based on biological or anatomical models of what a face–or the features that make up a face—look like. Instead, the algorithm performance is entirely dependent upon the patterns which the algorithm developer finds to be most useful for finding similarities. The patterns used in AFR algorithms do not correlate to obvious anatomical features such as the eyes, nose or mouth in a one-to-one manner, although they are affected by these features.

Biometric Template—A biometric template is a set of biometric measurement data [or features] prepared by a face recognition system from a face image.[1] The prepared set can be compared to a probe image. An enrolled image, on its own, is not a biometric template. See Features.

Biometrics—A general term used alternatively to describe (1) a characteristic or (2) a process—(1) a measureable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition or (2) automated methods of recognizing an individual based on measureable biological (anatomical and physiological) and behavioral characteristics.[2]

Candidates—See Candidate Images.

Candidate Images—The possible results of a face recognition search. When face recognition software compares a probe image against the images contained in a repository (See Repository.), the result is a list of most likely candidate images that were determined by the software to be sufficiently similar to or most likely resemble the probe image to warrant further analysis. A candidate image is an investigative lead only and does not establish probable cause to obtain an arrest warrant without further investigation.

Candidate List—One or more most likely candidate images resulting from a face recognition search. See Candidate Images.

Center—See Fusion Center.

Civil Liberties—According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "civil liberties" refers to fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals.[3] They are the freedoms that are guaranteed by the Bill of Rights—the first 10 amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Civil Rights—The term "civil rights" refers to those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against on the basis of any federal- or state- protected characteristic. For example, a state may have constitutional or statutory language regarding parental status. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.[4]

Collect—For purposes of this document, "gather" and "collect" mean the same thing.

Comparison—The observation of two or more faces to determine the existence of discrepancies, dissimilarities, or similarities.[5] See Face Comparison.

Computer Security—The protection of information technology assets through the use of technology, processes, and training.

Confidentiality—Refers to the obligations of individuals and institutions to appropriately use information and data under their control once they have been disclosed to them and in accordance with applicable data security laws and policies. See Privacy.

Consent—In general use, consent means compliance in or approval of what is done or proposed by another; specifically, the voluntary agreement or acquiescence by a person of age or with requisite mental capacity who is not under duress or coercion and usually who has knowledge or understanding. Related to mobile

[1] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

[2] Ibid.

[3] *Civil Rights and Civil Liberties Protections Guidance*, at 4 (August 2008), https://www.dni.gov/files/ISE/documents/DocumentLibrary/Privacy/CR-CL_Guidance_08112008.pdf.

[4] The definition of "civil rights" is a modified version of the definition contained in the *National Criminal Intelligence Sharing Plan* (NCISP), at pp. 5–6. *Civil Rights and Civil Liberties Protections Guidance* (August 2008), https://www.dni.gov/files/ISE/documents/DocumentLibrary/Privacy/CR-CL_Guidance_08112008.pdf.

[5] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

face recognition, consent means an individual agrees to have his or her image taken by a law enforcement officer for purposes of identification. See Revocation.

Continuous Monitoring—A system security process that comprises ongoing situational awareness of information security, vulnerabilities, threats, and incidents for each user level to support entity risk management decisions.

Credentials—Information that includes identification and proof of identification that are used to gain access to local and network resources. Examples of credentials are usernames, passwords, smart cards, and certificates.

Criminal Activity—A behavior, an action, or an omission that is punishable by criminal law.

Criminal Case Support—Administrative or analytic activities that provide relevant information to law enforcement personnel regarding the investigation of specific criminal activities or trends or specific subject(s) of criminal investigations.

Criminal Intelligence Information—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

Data—Inert symbols, signs, descriptions, or measures; elements of information.

Data Breach—The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information (PII) or (2) an authorized user accesses or potentially accesses PII for a purpose other than authorized purposes. An entity's response to a data breach may be addressed in state law or agency policy. This may include incidents such as:

- Theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted.
- Posting such information on the internet.
- Unauthorized employee access to certain information.
- Moving information to a computer otherwise accessible from the internet without proper information security precautions.
- Intentional or unintentional transfer of information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail.
- Transfer of information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

Data Quality—Refers to various aspects of the information, such as the accuracy and validity of the actual values of the data, information structure, and database/information repository design. Traditionally, the basic elements of data quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, data quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy. This concept is also addressed as one of the Fair Information Practice Principles (FIPPs), Data Quality/Integrity. See Appendix B for a full set of FIPPs.

Direct Face Recognition Collection—The entity is owner of the face recognition equipment that captures face recognition information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of PII in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Dissemination—See Disclosure.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, compact disc optical media, or cloud technologies.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as movement of information from one location to another by magnetic or optical media, or transmission over the internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Enhancement—Image enhancement is the process of adjusting digital images so that the results are more suitable for display or further image analysis. For example, removing noise, sharpening or brightening an image may make it easier to identify key features.

Enroll—The process of storing and maintaining information. Specifically in the face recognition context, biometric enrollment is capturing a face image, creating a biometric template from the image, and entering the template into a face recognition repository.[6] See Biometric Template and Repository.

Enrolled Image—An image that is loaded to, and may be stored in, an image repository (see Repository) and used as a reference image for face recognition comparisons (searches). Enrolled images do not include probe images. Some images of individuals may not be enrolled because they do not meet established criteria.

Enrollment—See Enroll.

Entity—The **[name of entity],** which is the subject and owner of the face recognition policy.

Evaluation—Refer to Image Evaluation.

Examiner—An individual who has received advanced training in the face recognition system and its features. Examiners have at least a working knowledge of the limitations of face recognition and the ability to use image editing software. They are qualified to assess image quality and appropriateness for face recognition searches and to perform one-to-many and one-to-one face image comparisons.

Examiners determine if probe images are suitable for face recognition searches, and may enhance images for the purpose of conducting a face recognition search. Though enhancements to the probe image are permissible, the examiner does not base any conclusions on a comparison between an enhanced probe image and a potential candidate photo. Examiners shall evaluate search results by comparing the original unknown probe image with the potential candidate photo.

Expression—Facial aspects resulting from muscle movement or position.[7]

Face Comparison—The manual examination of the differences and similarities between two face images or a live subject and a face image (one-to-one) for the purpose of determining if they represent the same or different persons.[8] See Face Recognition, One-to-One Face Image Comparison, and Verification.

Face Detection—Automated determination of the locations and sizes of human faces in digital images.[9]

Face Examiner—See Examiner.

Face Recognition—The automated searching for a reference image in an image repository (see Repository) by comparing the facial features of a probe image with the features of images contained in an image repository (one-to-many search). A face recognition search will typically result in one or more most likely candidates—or candidate images—ranked by computer-evaluated similarity or will return a negative result. See Candidate Images.

Face Recognition Program—An entity's face recognition initiative that includes the management of human components (management, analysts, examiners, authorized users), ownership and management of the face recognition system (technical components), and the establishment and enforcement of entity-wide processes, policies, and procedures. See Face Recognition System.

Face Recognition Software/Technology—Third-party software that uses specific proprietary algorithms to compare facial features from one specific picture—a probe image—to many others (one-to-many) that are stored in an image repository (see Repository) to determine most likely candidates for further investigation. See Candidate Images.

Face Recognition System—The technical components of a face recognition program, such as hardware, software, interfaces, image repositories, biometric templates, autogenerated candidate lists, etc. While some entities own such a system, others may only have authorized access to another entity's face recognition system. See Face Recognition Program.

Facial Recognition—See Face Recognition.

Fair Information Practice Principles—The Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies both within government and the private sector. Although specific articulations of FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into information privacy

[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] Ibid.

laws, policies, and governance documents around the world. They provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal use that needs to be done with regard to privacy in integrated justice systems. Because of operational necessity, it may not always be possible to apply all of the principles equally. For example, the Individual Participation Principle (#8) may be of limited applicability in intelligence operations, as entities do not generally engage with individuals and under federal law, the Privacy Act of 1974 contains exemptions in the law enforcement context. That said, law enforcement entities and all other integrated justice systems should endeavor to apply FIPPs where practicable and ensure compliance with applicable law.

The eight principles are:

1. Purpose Specification
2. Data Quality/Integrity (See definition.)
3. Collection Limitation/Data Minimization
4. Use Limitation
5. Security Safeguards (See definition.)
6. Accountability/Audit
7. Openness/Transparency
8. Individual Participation

See Appendix B for one description of how the U.S. Department of Homeland Security applies these principles.

Features—Observable class or individual characteristics. The components of biometric templates. [10]

Filtering—In the face recognition context, filtering uses relevant physical facial attributes such as eye color, nose shape, eyebrow position, hairline, and other attributes to compare, select, and narrow results. See Attributes.

Firewall—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

Frontal Pose—A face image captured from directly in front of the subject with the focal plane approximately parallel to the plane of the subject's face.[11]

Fusion Center—A fusion center is a collaborative effort of two or more federal, state, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity.[12] State and major urban area fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between federal and SLTT government agencies and private-sector partners.

Holistic Comparison—The process of comparing faces by looking at the face as a whole and not the component parts in isolation.[13]

Identity—Within a biometric system, the collective set of biographic data, images, and biometric templates assigned to one person.[14] See Face Comparison.

Image—See Probe Image and Repository.

Image Analysis—The assessment of an image to determine suitability for comparison, including the ability to discriminate significant features.[15]

Image Enhancement—See Enhancement.

Image Evaluation—Ascertaining the value of dissimilarities and similarities between two face images, where an examiner assesses the value of the details observed during the analysis and comparison steps and reaches a conclusion.[16]

Image Repository—See Repository.

Individual Characteristics—Characteristics allowing one to differentiate between individuals having the same class of characteristics (e.g., freckles, moles, and scars).[17]

Individual Responsibility—Because a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

Individualization—The determination by an examiner that there is sufficient agreement in the quality and quantity of detail to conclude that two

[10] Ibid.

[11] Ibid.

[12] ISE-SAR Functional Standard, version 1.5.5. Source: Section 511 of the 9/11 Commission Act.

[13] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] Ibid.

images depict the same person.[18] Such results are generally referred for peer and supervisory reviews and approval before any dissemination of results is made.

Information—Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into three general areas: general data, including investigative information; tips and leads data, including suspicious activity reports; and criminal intelligence information.

Information Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

Information Quality (IQ)—Refer to Data Quality.

Information Sharing Environment (ISE)—In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the Information Sharing Environment (ISE) is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of SLTT agencies, federal agencies, and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

Intelligence—See Criminal Intelligence Information.

Invasion of Privacy— Intrusion on an individual's solitude or into an individual's private affairs, public disclosure of embarrassing private information, publicity that puts an individual in a false light to the public, or appropriation of an individual's name or picture for personal or commercial advantage. See also Right to Privacy.

Investigative Lead—Any information which could potentially aid in the successful resolution of an investigation, but does not imply positive identification of a subject or that the subject is guilty of a criminal act.

Known Image—The image of an individual associated with a known or claimed identity and recorded electronically or by other medium (also known as exemplars).[19] Known images are enrolled and stored in an image repository. See Repository.

Law—As used by this policy, law includes any local, state, or federal constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement (LE) Agency—An organizational unit, or subunit, of a local, state, federal, or tribal government with the principal functions of prevention, detection, and investigation of crime, apprehension of alleged offenders, and enforcement of laws. LE agencies further investigations of criminal behavior based on prior identification of specific criminal activity with a statutory ability to perform arrest functions.

Law Enforcement Information—For purposes of the ISE (see Information Sharing Environment), law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including, but not limited to, information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident—A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

Logs—A necessary part of an adequate security system which ensures that information is properly tracked and that only authorized individuals are getting access to the data. See also Audit Trail.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases or repositories) and nonelectronic storage systems (for example, filing

[18] Ibid.

[19] Ibid.

cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Manual Face Examination—Comparison and evaluations of the probe image and the candidate images by a trained biometric images specialist.

Match/Matching—For the purposes of face recognition, see Candidate Images.

Morphological Comparison—The direct comparison of class and individual face characteristics without explicit measurement.[20] See Comparison and Manual Face Examination.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information to perform or assist in a law enforcement, homeland security, or counterterrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement.

Nodal Points—Measurements of distinctive face characteristics, including, but not limited to, the distance between the eyes, width of the nose, and the depth of the eye sockets. Nodal points are extracted from the face image and are transformed through the use of algorithms into a unique file called a biometric template. See Biometric Template.

No Match—A negative result from a face recognition search in which the probe image was determined not to be sufficiently similar to or resemble any of the reference images contained in an image repository.

Non-Criminal Justice Agency—An entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

One-to-Many Face Image Comparison—The process whereby a probe image from one subject is compared with the features of reference images contained in an image repository, generally resulting in a list of most likely candidate images (one-to-many). See Candidate Images.

One-to-One Face Image Comparison—The process whereby a probe image from one subject is compared with a most likely candidate image that is also from one subject (one-to-one). See Comparison, Face Comparison, and Verification.

Participating Agency—An organizational entity that is authorized to contribute images and/or biometric information to a face recognition system and/or is authorized to access or receive, request, or use face recognition information from the **[name of entity]**'s face recognition system for lawful purposes through its authorized individual users. Participating agencies adhere to conditions defined in a formal agreement (e.g., MOU or interagency agreement) between the **[name of entity]** operating the face recognition program and the participating agency.

Peer Review—An additional layer of verification of face recognition results in a face recognition search process. Examiners submit face recognition search results to other authorized and trained examiners—or peers—for an independent review and cross-verification of the probe and most likely candidate images. If verified by peer(s), this step is generally followed by a supervisor's review and approval prior to dissemination. Refer to Verification.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, a directory, or a printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personally Identifiable Information (PII)—
Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information, that is linked or linkable to a specific individual." [21]

Pose—The orientation of the face with respect to the camera, consisting of pitch, roll, and yaw. Common poses are frontal and profile.[22]

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of PII. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the

[20] Ibid.

[21] For further information about the breadth of PII and how to perform an assessment of the specific risk that an individual can be identified using the information, see Revision of Office of Management and Budget Circular A-130: Managing Information as a Strategic Resource, July 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.

[22] Ibid.

capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); and to avoid being seen or overheard in particular contexts.

Privacy Policy—Short term for a privacy, civil rights, and civil liberties (P/CRCL) policy which is a printed, published statement that articulates the policy position of an organization on how it handles the PII that it gathers or receives and uses in the normal course of business. The policy should include information relating to the processes of information collection, receipt, access, use, dissemination, retention, and purging. It is likely to be informed by the FIPPs. The purpose of the P/CRCL policy is to articulate that the entity will adhere to those legal requirements and entity policy determinations that enable collection, receipt, access, use, dissemination, retention, and purging of information to occur in a manner that protects personal privacy interests. A well-developed P/CRCL policy uses justice entity resources wisely and effectively; protects the entity, the individual, and the public; and promotes public trust.

Probe Image—Any face image used by face recognition software for comparison with the face images contained within a face image repository. See Repository.

A front-facing image of an individual lawfully obtained pursuant to an authorized criminal investigation. Examples of probe images include:

- Face images captured from closed circuit TV cameras
- Face images captured from an ATM camera
- Face images provided by a victim or witness of a crime
- Face images gained from evidence (fraudulent bank card or photograph ID)
- Face sketches (for example, police artist drawings)

Protected Information—For the nonintelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States.

For the (federal) intelligence community, protected information includes information about “United States persons” as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, policy, or other similar instrument.

For state, local, tribal, and territorial governments, protected information may include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, tribal, and territorial laws, ordinances, and codes. Protection may be extended to other individuals and organizations by a law enforcement entity or other state, local, tribal, or territorial agency policy or regulation.

Public—Includes:

- Any individual and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the entity’s information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit and without distinction as to the nature or intent of those requesting information from the entity or participating entity.

Public does not include:

- Any employees of the entity or participating entity.
- People or entities, private or governmental, who assist the entity in the operation of the justice information system.
- Public entities whose authority to access information collected or received and retained by the entity is specified in law.

Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Purge—A term that is commonly used to describe methods that render data unrecoverable in a storage space or destroy data in a manner that it cannot be reconstituted. There are many different strategies and techniques for data purging, which is often contrasted with data deletion (e.g., made inaccessible except to system administrators or other privileged users).

Recognition—See Face Recognition.

Record—Any item, collection, or grouping of information that includes PII and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting agency or organization.

Redress—Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding *protected information* about them which is under the entity's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

Protected information includes personal information about individuals that is subject to information privacy or other legal protections by law. Protection may also be extended to organizations by entity policy or state, local, tribal, or territorial law.

Relative Frequency—How often facial features or combinations thereof occur in a given population.[23]

Repository—A location where a group of images of known individuals and biometric templates are stored and managed. An image repository is searched during a face recognition search process whereby a probe image is used by face recognition software for comparison with the images (or features within images) contained in the image repository.

Request—A request received by the **[name of entity]** to utilize face recognition in support of a criminal investigation. Submissions will not contain original evidence. Images received in a request or submission will not be stored as enrolled images within the face recognition system.

Retention—See Storage.

Revocation—In general use, revocation is the act of recall or annulment. It is the reversal of an act, the recalling of a grant or privilege, or the making void of some deed previously existing. As it relates to the revocation of consent to be photographed or the individual's image captured by a law enforcement officer to perform a mobile face recognition search for purposes of identification, once consent to capture an individual's image is given, an individual may withdraw consent with an unequivocal act or statement of withdrawal. Consent may be withdrawn by statements, actions, or a combination of statements and actions. However, the revocation of consent must clearly be a statement revoking consent; an expression of impatience or dislike is not sufficient to terminate consent.

Revoke—See Revocation.

Right to Information Privacy—The right to be left alone, in the absence of some reasonable public interest in collecting, accessing, retaining, and disseminating information about an individual's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the individual or entity violating an individual's privacy.

Right to Know—A requirement for access to specific information to perform or assist in a lawful and authorized government function. Right to know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity, or the roles and responsibilities of particular personnel in the course of their official duties.

Role-Based Access—A type of access authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

Search—For the purposes of face recognition, the act of comparing a probe image against an image repository.[24] See Repository.

Search Filters—See Filtering.

Search Result Set—The candidate list returned from a face recognition search.[25] See Candidate Images.

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of information for the legitimate user set, as well as promoting failure resistance in the electronic systems overall. Security safeguarding of information is a Fair Information Practice Principle (FIPP). See Appendix B.

Source Entity—Refers to the entity or organizational entity that originates face recognition information.

Storage—In a computer, storage is the place where data is held in electromagnetic or optical form for access by a computer processor. There are two general usages:

- Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-

[23] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

[24] Ibid.

[25] Ibid.

computer storage. This is probably the most common meaning in the IT industry.

- In more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called "random access memory," or RAM) and other built-in devices, such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations. Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

Submission—See Request.

System Bias—Errors repeatedly introduced through automation (e.g., errors in biometric template generation or comparison). Errors repeatedly introduced through operational practices in an organization or unit (e.g., improper lighting or camera position guidance).[26]

Template—See Biometric Template.

Uncontrolled Image—An image for which the subject did not pose (e.g., security camera images, cell phone photograph taken by a witness).

Unsolved Image File—A lawfully obtained probe image of an unknown suspect *may* be added by authorized law enforcement users to an unsolved image file pursuant to an authorized criminal investigation and if a search has produced no candidates and the subject remains unknown. Images in an unsolved image file are periodically compared with the known images in an image repository. Images enrolled in an unsolved image file should be required to be validated periodically by the contributors to ensure that the criminal investigation remains active and that the image remains relevant to the investigation.

User—An **[name of entity]** employee or an individual representing a participating agency who is authorized and trained to access and use, or receive results from, an entity's face recognition system for lawful purposes.

Valid Law Enforcement Purpose—A purpose for information/intelligence gathering, development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, protection of public or private structures and property, furthering officer safety (including situational awareness), and homeland and national security, while adhering to law and agency policy designed to protect the P/CRCL of Americans.[27] Similar terms include "reasonable law enforcement purpose,"[28] "legitimate law enforcement purpose," and "authorized law enforcement activity."[29]

Verification—In a biometric system, the process of conducting a one-to-one comparison. A task where the face recognition system attempts to confirm an individual's claimed identity by comparing the biometric template generated from a submitted face image with a specific known template generated from a previously enrolled face image.

A review and independent analysis of the conclusion of another examiner.[30]

[26] Ibid.

[27] See *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*, Global, BJA, OJP, DOJ, February 2013, https://it.ojp.gov/GIST/132/Developing-a-Policy-on-the-Use-of-Social-Media-in-Intelligence-and-Investigative-Activities--Guidance-and-Recommendations- and also in the *Real-Time and Open Source Analysis (ROSA) Resource Guide*, Criminal Intelligence Coordinating Council (CICC), Global, BJA, OJP, DOJ, July 2017, https://it.ojp.gov/GIST/1200/Real-Time-and-Open-Source-Analysis--ROSA--Resource-Guide (using "valid law enforcement purpose").

[28] *Recommendations for First Amendment-Protected Events for State and Local Law enforcement Agencies*, CICC, Global, OJP, DOJ, and DHS, December 2011, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

[29] The term "authorized law enforcement activity" is used, for example, in *The Attorney General's Guidelines For Domestic FBI Operations*, as provided in sections 509, 510, 533, and 534 of title 28, United States Code, and Executive Order 12333, September 29, 2008.

[30] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

Appendix B

Disclaimer:

As a condition to the use of this document and the information contained herein, the Facial Identification Scientific Working Group (FISWG) requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that FISWG be notified as to its use and the outcome of the proceeding. Notifications should be sent to: chair@fiswg.org

Redistribution Policy:

FISWG grants permission for redistribution and use of all publicly posted documents created by FISWG, provided that the following conditions are met:

Redistributions of documents, or parts of documents, must retain the FISWG cover page containing the disclaimer.

Neither the name of FISWG, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a FISWG document must include the version number (or creation date) of the document and mention if the document is in a draft status.

Version 2.0 2020.07.17

Standard Practice/Guide for Image Processing to Improve Automated Facial Recognition Search Performance

1. Scope

1.1 The purpose of this document is to provide guidelines for processing a probe image in order to increase the likelihood that a potential candidate will be included among the search result set returned following a facial recognition system (FRS) search.

1.1.1 This process is not suitable for developing source conclusions regarding an image.

1.1.2 The guideline does not address the necessary steps and processes for that type of examination.

2. Referenced Documents

2.1 *ASTM* Standards:

E2916 Terminology for Digital and Multimedia Evidence Examination[1]

E2825 Standard Guide for Forensic Digital Image Processing

2.2 Other Standards:

ANSI/NIST- ITL-1-2011 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information[2]
FISWG Facial Recognition Systems Metadata Usage[3]

[1] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@asstm.org. For Annual Book of ASTM Standards volume information, refer to the standard's Document Summary page on the ASTM website.

[2] For referenced ANSI/NIST documents, visit https://www.nist.gov/programs-projects/ansinist-itl-standard

[3] For referenced FISWG documents, visit https://fiswg.org/documents.html

3. Terminology

3.1 Definitions: See ASTM E2916 Terminology for digital and multimedia evidence examination terms.

3.1.1 Lossy compression - data reduction process that is not completely reversible, and some original data is irretrievably lost

3.1.2 Lossless compression - a data reduction process that is completely reversible, such that all of the original data can be retrieved in the original form.

3.1.3 Pixel aspect ratio - the ratio of the width to the height of a rectangle, such as an image, a pixel, or an active video frame.

3.2 Acronyms

FRS - Facial Recognition Systems

4. Summary of Guide

The image processing steps presented in this document are limited to the manual processing of images intended to be submitted as probe images for FRS searches. Internal image processing applied by the FRS and issues associated with still image extraction from video, scanning of printed imagery, and the use of forensic sketches, reconstructions, and composites are beyond the scope of this document.

5. Significance and Use

5.1 **Introduction**

Images that meet agreed upon international standards (such as ISO/IEC 19794-5: Face Image Data[4]) can normally be submitted to an FRS for searching with little or no operator intervention. Many FRS also include intrinsic mechanisms for correcting minor deviations in subject pose, image size, or vendor specific adjustments to the image. Manual processing may be beneficial for sub-optimal images (e.g. low resolution, heavily compressed or where the subject’s pose, illumination, or expression is non-neutral). The image processing techniques presented in this document may be applied over an entire image or in localized areas of an image.

[4] Available from https://www.iso.org/standard/38749.html

The image processing topics presented in this document are not intended to override recommendations for maintaining the quality of images intended for one-to-one comparison. These processes specifically apply to the preparation of a facial image for the purpose of submitting it as a probe into an automated FRS search to maximize the likelihood that a potential candidate will be returned in the search result set. These processes are not to be used for identification purposes.

5.2 **Important Notes**

5.2.1 The goal of any image processing should be to optimize the image for searching by the FRS, not to create an aesthetically pleasing image. An image that looks ‘good’ is not necessarily the same as one that is optimized for use by an FRS due to image processing done within the vendor specific algorithms.

5.2.2 The effect of any manual image processing will vary with different FRS and in some cases may degrade performance rather than improve it.

5.2.3 Image processing to the probe image before an FRS search is different from the operational processes performed for the purpose of a one-to-one manual comparison.

5.2.4 Any decision regarding whether or not a candidate returned from an FRS search is from a possible common source as the subject in the probe image must be made based on a comparison with the original (unedited) image and NOT the processed image.

5.2.5 Agency specific or mandated notes and audit trails shall be done at all times. Document and preserve processed images regardless of search results.

The following sections of this document describe a series of steps with varying complexity for the manual processing of probe images of less than optimal quality for an FRS. They are intended to maximize the likelihood of returning a potential candidate from a search result set while minimizing the amount of processing of the probe image. Guidelines presented in this document may be adapted for agency specific policies and standard operating procedures.

6. Procedure

6.1 **Initial Steps**

The initial steps for the management of probe imagery include, but are not limited to, the following:

6.1.1 Save original

The original untouched probe image should be kept in all cases. A read-only copy shall be made of the original probe image(s). No enhancements or modifications shall be made to these original probe image(s). When making any final comparisons, always use a working copy of the original probe image(s).

6.1.2 Make lossless working copies

All image processing steps should be done using a lossless file format.

Understanding the compatibility of image file formats for an FRS is critical because the original image(s) may be received in a variety of file formats. If a probe image is not in an FRS compatible format, follow the vendor's recommendations for conversion to a supported compatible format. This conversion (if needed) should be done as a last step from the lossless images being processed, prior to searching.

6.2 **Generalized Search Steps**

For the purpose of this document, "pass" refers to an assumption that following each progression of image processing, an FRS search will take place and the resulting candidates will be assessed. It may not be prudent to run the probe image through an FRS search until it has been processed to a certain degree. In all examples of "passes" presented in this document it is assumed that for every sequential "pass", the following steps shall be undertaken in every FRS search of a probe image. See Figure 1 below: **Simplified Image Processing Flow Chart**.

6.2.1 Verify eyes can be found. This step can also be described as "localizing the face in the image". This is critical to determine if the facial imagery utilized has limitations or systemic image conditions, which may cause a problem when submitting to the proprietary technology within an FRS.

6.2.2 Save interim image sets – All processed images used for searching shall be saved according to agency policy. Searching images with different enhancements (e.g. cropped, black and white, or grayscale) may result in different candidate sets.

6.2.3 Search and review results – FRS results shall be compared against the original probe image(s). If no potential candidates are returned in the search result set, the recommendation is to re-evaluate the image that was used in searching and apply further processing.

6.2.4 If available within the FRS, consider using metadata binning. The FISWG document ***Facial Recognition Systems Metadata Usage***[5] should be referenced where metadata is accessible which refines searches through reducing the logical size of the search database.

[5] Available from: https://www.fiswg.org/documents.html

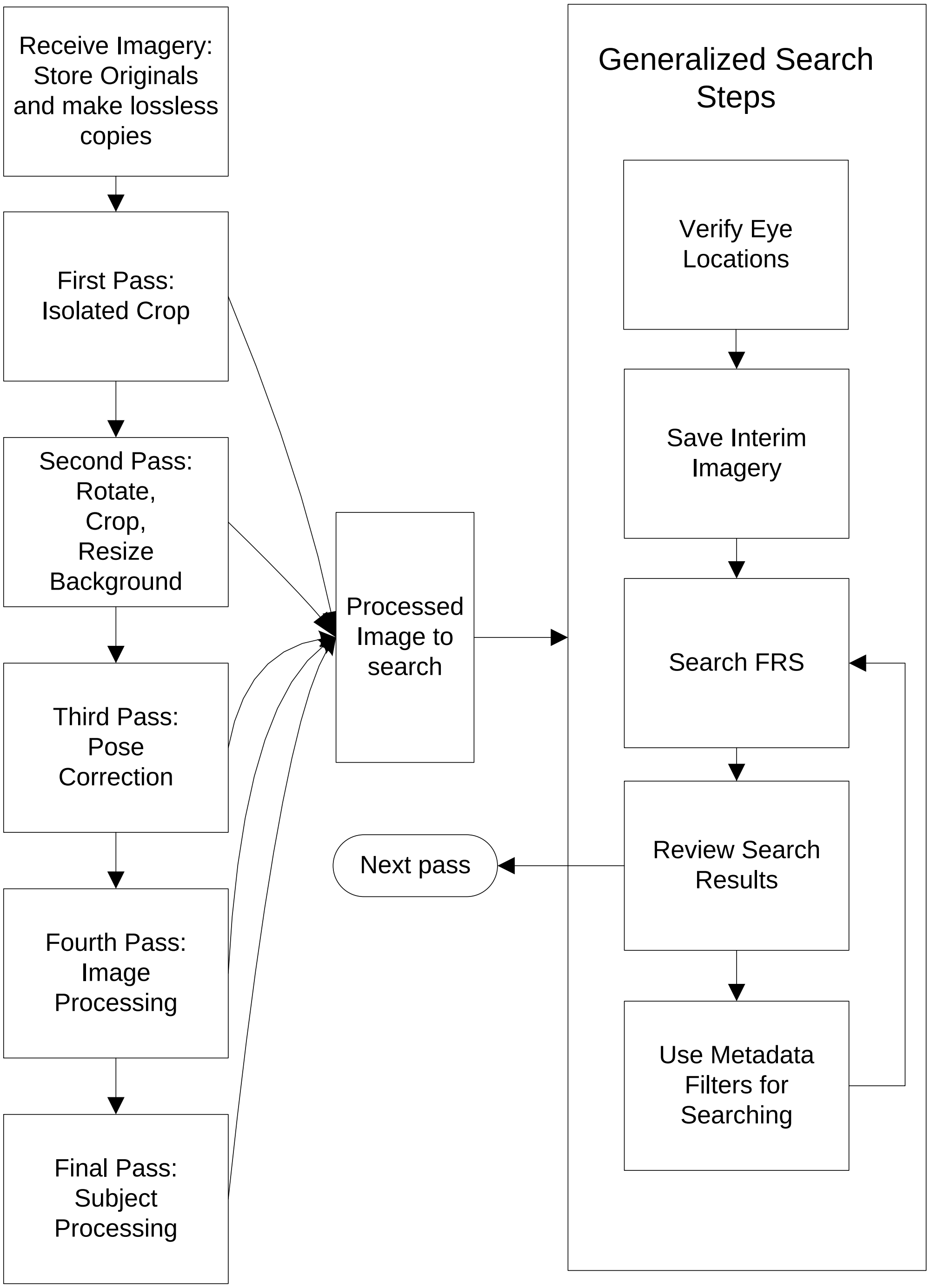

Receive Imagery: Store Originals and make lossless copies
First Pass: Isolated Crop
Second Pass: Rotate, Crop, Resize Background
Third Pass: Pose Correction
Fourth Pass: Image Processing
Final Pass: Subject Processing
Processed Image to search
Next pass
Generalized Search Steps
Verify Eye Locations
Save Interim Imagery
Search FRS
Review Search Results
Use Metadata Filters for Searching

Figure 1: Simplified Image Processing Flow Chart

6.3 **First Pass: Isolated Crop**

The First Pass should be initiated with the original image. The relevant face(s) should be cropped, if not undertaken automatically by the FRS. When cropping, ensure that the aspect ratio is maintained and aim to produce an image that is in accordance with ANSI/NIST- ITL-1-2011or ISO specifications.

6.4 **Second Pass: Rotate, Crop, Resize, Background**

The Second Pass would be initiated when no potential candidates are found during the First Pass or when the nature of the image warrants minimal processing to yield additional candidates.

The Second Pass may include the tasks below, all of which are not necessarily required; however, if more than one is applied, they should be performed one at a time. When processing images, care should be taken to not remove or alter portions of the subject's head (e.g. portions of the ear, crown of the head, or portions of the neck).

6.4.1 Rotate – The image may be rotated around the roll axis to make the eye positions appear horizontally aligned.

6.4.2 Secondary Crop – The image processing steps done in this pass may require a secondary crop of the image. The goal of this crop is to produce an image that is more in accordance with the ANSI/NIST- ITL-1-2011or ISO specifications.

6.4.3 Resize – Modify the size of the image to achieve a recommended interpupillary distance. This distance should be agency defined and based on FRS vendor recommendations (e.g. 90 pixels). Resizing of the images should be done in even multiples of the original image size while preserving the original image aspect ratio. For example: 90x120 pixels to 180x240 pixels to 270x360 pixels, etc.

6.4.4 Blur background – This is performed where the probe image has a non-neutral or busy background. The blurring process creates a consistent background preventing an FR engine from detecting items in the background. Examples include:

6.4.4.1 Surveillance photo with people or items in background.

6.4.4.2 An image captured with a background that varies in color and content.

6.4.5 Horizontal flip – This should be utilized if the probe image submitted may have been taken as a reflection, captured incorrectly, or been flipped left/right or right/left in transmission.

6.4.6 Aspect ratio correction – mitigates the impact of an image that looks unnaturally stretched in the horizontal or vertical direction.

6.5 Third Pass: Pose Correction

FRS algorithms have varying sensitivities to non-frontal facial imagery. Claims of performance degradations will vary, but it is broadly accepted that any non-frontal pose movements could negatively affect FRS performance.

The standard definitions of pose angles are defined in: **NIST Special Publication 500-290 Edition 3 (2015)** and **ANSI/NIST-ITL 1-2011 Update: 2015 Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information**[6] as referenced in Figure 2:

[6] Available from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-290e3.pdf

The Yaw and Roll angles shall be measured from the full face pose position and have a range of values from -180 degrees to +180 degrees. The Pitch angle shall have a range of values from -90 degrees to +90 degrees. The pose angle set is given by Tait-Bryan angles as shown in Figure 26.

ANSI/NIST-ITL 1-2011: UPDATE 2015

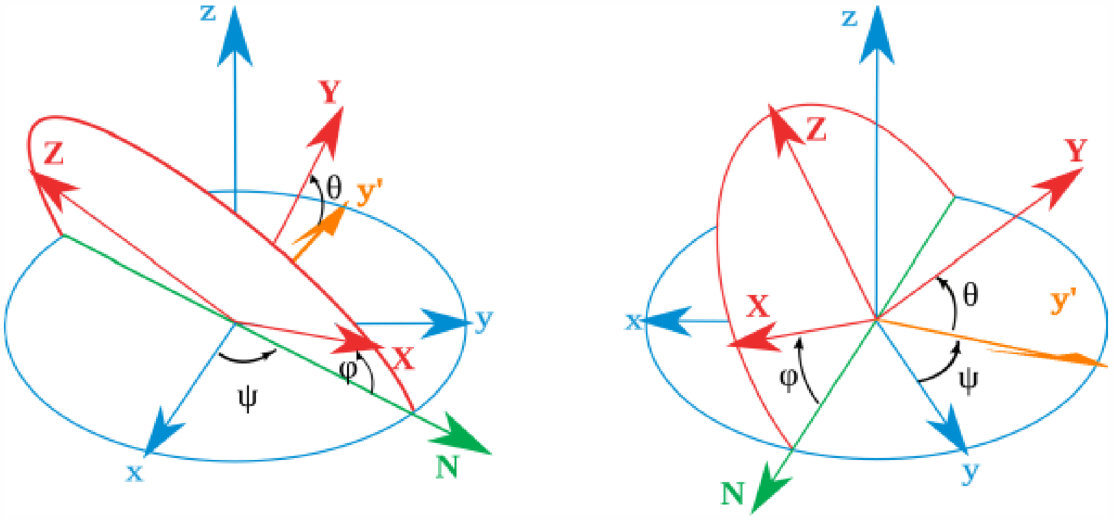


Figure 26: Tait-Bryan angles statically defined with the Z-X'-Y'' convention

The angles are defined relative to the frontal view of the subject, which has angles (0, 0, 0). Examples are shown in Figure 27.

Yaw angle: rotation about the vertical (y) axis. A positive Yaw angle is used to express the angular offset as the subject rotates from a full-face pose to his or her left (approaching a right profile). A negative Yaw angle is used to express the angular offset as the subject rotates from a full-face pose to his or her right (approaching a left profile).

Roll angle: rotation about the horizontal side-to-side (z) axis.

Pitch angle: rotation about the horizontal back to front (x) axis.

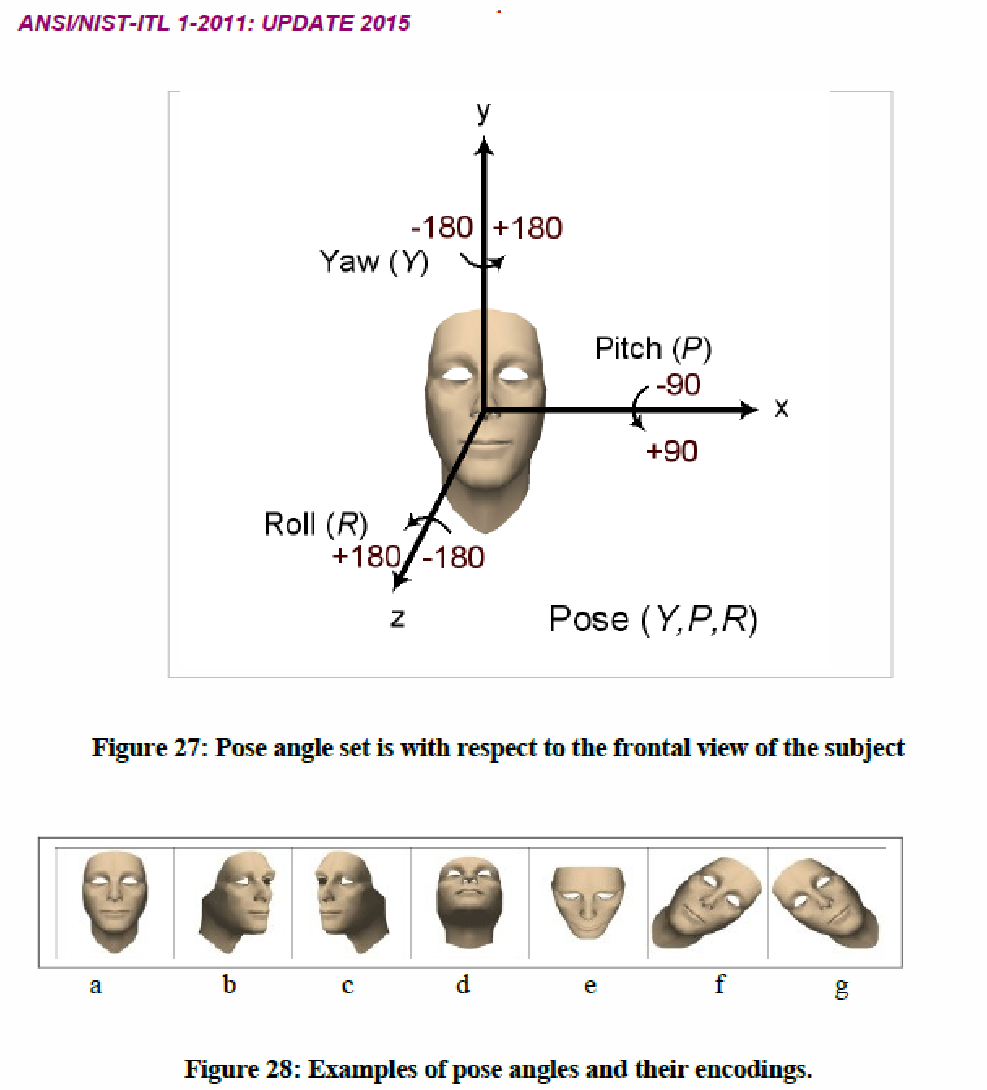

ANSI/NIST-ITL 1-2011: UPDATE 2015

Figure 27: Pose angle set is with respect to the frontal view of the subject

Figure 28: Examples of pose angles and their encodings.

The pose angles (Y, P, R) of (a) – (g) in Figure 28 are given by (0, 0, 0), (+45, 0, 0), (-45, 0, 0), (0, -45, 0), (0, +45, 0), (0, 0, -45), and (0, 0, +45), respectively.

The uncertainty in the pose angles is given by the range 0 to 90, inclusive. It shall denote approximately a maximum value of possible deviation in the measurement of the pose. This shall correspond to a two standard deviation confidence interval.

The encoding of angles is in ASCII format, with the minus sign “-“ used to denote a negative value and the plus “+” sign optionally used to denote a positive value. Pose angle uncertainty angles are always positive.

Figure 2: NIST Special Publication 500-290 Edition 3 (2015)

6.5.1 Software for pose correction is dependent on policy or vendor recommendations. Any pose which varies more than 10 degrees in any direction from (0, 0, 0) could be considered a candidate for pose correction.

6.5.2 When pose correction is done, consideration shall be given to the following areas:

6.5.2.1 If available select the proper gender and race

6.5.2.2 Select any symmetric fill option

6.5.2.3 Place appropriate facial landmarks as needed

6.5.2.4 Select the number of poses to generate

6.5.2.4.1 Frontal

6.5.2.4.2 Slight left and right pose (e.g. +/- 15 degrees yaw)

6.5.2.4.3 Slight up and down pose (e.g. +/- 15 degrees pitch)

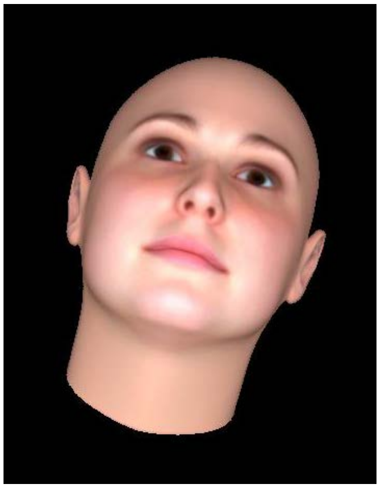
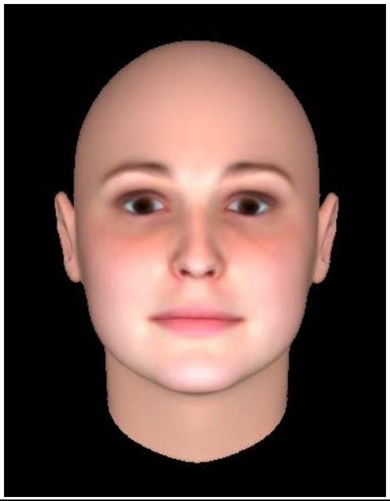
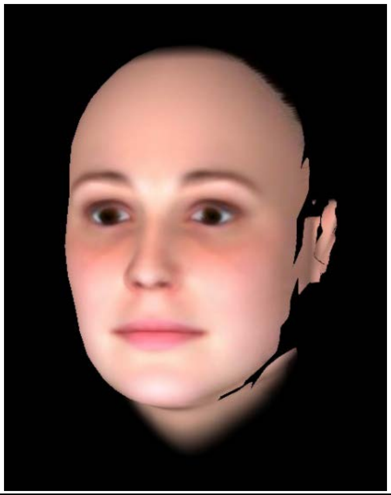
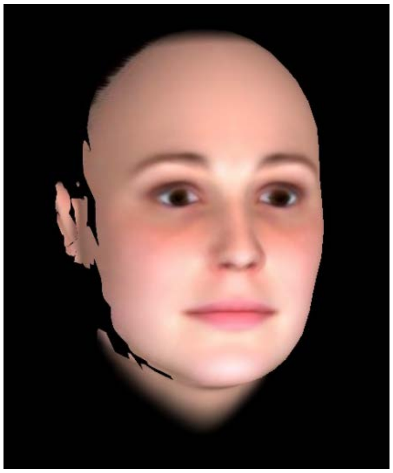
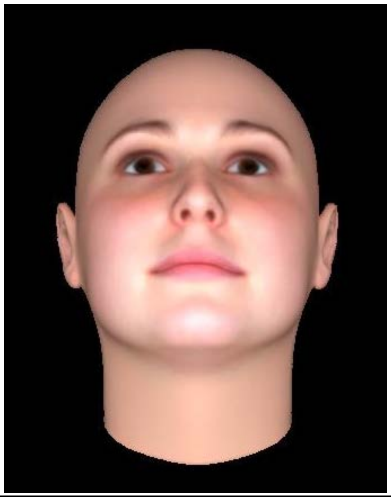
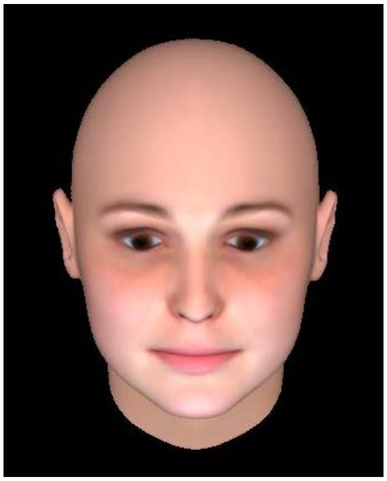
Pose	Example Image	Pose	Example Image
Original image		Pose corrected frontal	
Yaw -15 degrees		Yaw +15 degrees	
Pitch +15 degrees		Pitch -15 degrees	

Figure 3: Pose Examples

6.5.3 When multiple poses are generated, searching each pose as individual probe images within unique searches may allow for pose variations within the gallery. Some FRS supplied search clients allow group searching where groups of related imagery can be searched and reviewed in bulk.

6.6 **Fourth Pass: Image Processing**

6.6.1 During the Fourth Pass, image processing may be applied to a working copy of the original image or an image resulting from any of the previous passes to attempt to produce a different candidate search result set.

6.6.2 Image processing may be performed externally of the FRS using widely available image editors (e.g. Adobe Photoshop and GNU Image Manipulation Program [GIMP]) with the resulting probe image being submitted for an FRS search. The image processing listed below may be applied to the entire image or to selected regions within the image and may include, but are not limited to:

6.6.2.1 Histogram equalization

6.6.2.2 Color/tint corrections

6.6.2.3 De-blurring or sharpening

6.6.2.4 Lens distortion correction

6.6.2.4.1 Some images, such as those from smart phones, automated teller machines (ATM's) and Body Worn Video cameras that use wide-angle lenses typically exhibit perspective ('barrel') distortion. Image processing software or manufacturers' provided lens correction data should be used to correct this prior to searching.

6.6.2.5 Grayscale conversion

6.6.2.6 Noise reduction

6.6.2.7 Brightness or contrast adjustment

6.6.2.8 Red eye reduction

6.7 **Advanced Topic: Subject Processing**

6.7.1 After previous passes have been completed (or rejected due to the nature of the image) additional processing steps targeted at the subject in the image may be used.

6.7.2 This type of processing may introduce external elements to the subject in the image. Agency procedures shall be followed to determine whether these measures can be applied to improve the likelihood of locating a potential candidate from an image returned in the candidate search result set from an FRS search.

Reminder: Any decision on whether a particular candidate from a search is from a possible common source as the probe image shall be made using the original (unedited) image.

6.7.3 Circumstances warranting this type of image processing include, but are not limited to, the following:

6.7.3.1 Facial landmarks obstructed by head coverings, accessories (e.g., jewelry or eyewear), hair, image artifacts, etc.

6.7.3.2 Missing or obstructed facial landmarks due to extreme pose or expression (including closed eyes)

6.7.3.3 Intentional alterations of the subject’s face (e.g., excessive make-up)

6.7.3.4 Trauma (e.g., lacerations, blood, bruising), evidence of medical intervention (e.g., bandages, endotracheal tube, neck brace), or postmortem.

6.7.4 Examples of subject image processing include, but are not limited to, the following:

6.7.4.1 Replace or create missing facial landmarks on the subject.

6.7.4.2 Mirroring the probe image on the center line of the half face.

FISWG documents can be found at: www.fiswg.org

Appendix C

Disclaimer:

As a condition to the use of this document and the information contained herein, the Facial Identification Scientific Working Group (FISWG) requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that FISWG be notified as to its use and the outcome of the proceeding. Notifications should be sent to: chair@fiswg.org

Redistribution Policy:

FISWG grants permission for redistribution and use of all publicly posted documents created by FISWG, provided that the following conditions are met:

Redistributions of documents, or parts of documents, must retain the FISWG cover page containing the disclaimer.

Neither the name of FISWG, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a FISWG document must include the version number (or creation date) of the document and mention if the document is in a draft status.

Version 1.0   2020.12.11

Minimum Guidelines for Facial Image Comparison Documentation

1. Scope

1.1 The purpose of this document is to provide minimum guidelines and a common baseline of information for facial image comparison documentation.

1.1.1 Documentation may be in the form of notes, images with markups and annotations, narratives, worksheets, electronic records, investigative lead or forensic reports, or any combination of these methods.

1.2 This document does not discuss methods for how to conduct a facial image comparison, conclusion scale(s), or details that may be agency specific.

2. Terminology

2.1 *Definitions*

2.1.1 *Forensic Report:* a document whose intent it is to provide information to assist a trier of fact (e.g., judge or jury).

2.1.2 *Investigative Lead Report:* a document whose intent it is to provide information to assist operational personnel (e.g., investigator, detective, or analyst).

3. Significance and Use

3.1 These guidelines should be used as a reference by the practitioner to adequately document the facial image comparison process.

3.2 This document outlines the information needed to provide a clear understanding of the process conducted during a facial image comparison to the recipient.

3.3 The sections below provide the recommended minimum guidelines for information that should be documented in accordance with the type of report and agency specific needs.

4. Items to Document for a Facial Image Comparison

These items are not presented in order of importance or priority.

4.1 Administrative Data

4.1.1 Case Identifier

4.1.2 Dates

4.1.2.1 Date Received

4.1.2.2 Date Searched/Compared

4.1.2.3 Date of Image Capture (if available)

4.1.3 Requestor(s)

4.1.3.1 Contact Information

4.1.4 Any Written/Verbal Correspondence

4.1.5 Relevant Case Information (if provided)

4.1.6 Organization Conducting Examination

4.1.6.1 Contact Information

4.1.6.2 Practitioner(s)

4.1.7 Details and Scope of the Request (if provided)

4.1.8 Origin of Images

4.1.9 Filename/Identifier of Images Received

4.1.10 Indication of whether a facial recognition (FR) search was conducted and results (if applicable)

4.1.10.1 Gallery Searched

4.1.10.2 Number of Candidates Returned (based on maximum number returned or threshold used)

4.1.10.3 Ranking of returned potential candidate(s) if returned list is not randomized

4.1.11 Disclaimer **–** Agencies should include in all facial image comparison reports their own disclaimer identifying the limitations of the comparison method used and the recommended usage of the report.

4.1.12 Reference to Comparison Method Used

4.1.13 Description of the disposition of original and derivative works (e.g., returned, or retained)

4.2 Analysis

4.2.1 Determination of image applicability in the context of the question (e.g., Question asked is: are these two people the same? However, the images of the two persons display a large age difference and were taken days apart, then the persons cannot be same.)

4.2.2 Indication of images that do or do not meet agency specific requirements for comparison

4.2.2.1 Explanation for determination that images do not meet agency specific requirements

4.2.3 Image Analysis Documentation (e.g., lighting conditions, image resolution, etc.)

4.2.4 Processed Image(s) (if applicable)

4.2.4.1 Filename/Identifier of Processed Image(s) (if applicable)

4.2.4.2 Steps Taken to Process Image(s)

4.3 Comparison

4.3.1 Documentation of the Comparison

4.3.1.1 Compare and document features of the face visible in each image, as defined in the ASTM E3149 Facial Image Comparison Feature List for Morphological Analysis.

4.3.1.2 A documented account of the compared features

4.3.2 Observed effects of imaging conditions and physical stability of facial components or component characteristics

4.3.3 A visual example of the compared facial images

4.4 Evaluation

4.4.1 Conclusion Scale Used

4.4.1.1 Definitions or information and interpretation of what drives a conclusion (if applicable)

4.4.2 Conclusion Reached

4.5 Verification

4.5.1 Verification Notation

4.5.2 If the examination is not verified by a second examiner, a disclaimer that the comparison is not verified must be included in the report.

5. Additional Information

5.1 In accordance with the Agency's data retention policies, the following should also be saved (hard/digital):

5.1.1 All Correspondence (e.g., email, case notes, reports, etc.)

5.1.2 Received Images

5.1.3 Processed Images

5.1.4 Chain of Custody

5.1.5 Disposition (if applicable)

5.2 There should be documentation within the agency on the following:

5.2.1 Algorithm

5.2.1.1 Vendor Name

5.2.1.2 Version

5.2.1.3 Specific Configurations

5.2.1.4 Date Implemented

5.2.2 Software

5.2.2.1 Vendor Name

5.2.2.2 Version

5.2.2.3 Specific Configurations

5.2.2.4 Date Implemented

5.3 Agency Accreditation

5.3.1 Reference to Agency Comparison Method

5.3.2 Reference to Agency Standard Operating Procedures (SOP)

5.4 Practitioner Qualifications

6. Referenced Documents

6.1 American Society for Testing and Materials (ASTM) International Standard[1] E3149 Facial Image Comparison Feature List for Morphological Analysis

6.2 FISWG Physical Stability of Facial Features of Adults

6.3 FISWG Guide for Role-Based Training in Facial Comparison

6.4 FISWG Standard Practice/Guide for Image Processing to Improve Automated Facial Recognition Search Performance

6.5 FISWG Facial Comparison Overview and Methodology Guidelines

6.6 OSAC Standard Framework for Developing Discipline Specific Methodology for ACE-V

FISWG documents can be found at: www.fiswg.org

[1] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

Appendix D

Disclaimer:

As a condition to the use of this document and the information contained herein, the Facial Identification Scientific Working Group (FISWG) requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that FISWG be notified as to its use and the outcome of the proceeding. Notifications should be sent to: chair@fiswg.org

Redistribution Policy:

FISWG grants permission for redistribution and use of all publicly posted documents created by FISWG, provided the following conditions are met:

Redistributions of documents, or parts of documents, must retain the FISWG cover page containing the disclaimer.

Neither the name of FISWG, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a FISWG document must include the version number (or creation date) of the document and mention if the document is in a draft status.

Facial Image Comparison Feature List for Morphological Analysis

1. Scope

1.1 This guide defines a set of facial components, characteristics, and descriptors to be considered during a morphological facial comparison.

1.2 This set of facial components, characteristics, and descriptors describes the facial features that may be visible and comparable between images.

1.3 This guide defines a standard set of facial components, characteristics, and descriptors that should be used for facial comparison.

1.4 This guide does not define the comparison process itself, just the feature set to be used during such comparisons.

1.5 This guide does not define a classification system to constrain how those descriptors shall be articulated as applied to samples.

2. Terminology

2.1 Definitions:

2.1.1 Characteristic descriptors, n - minutiae of the component characteristics.

2.1.2 Component characteristics, n - detailed features of the facial components.

2.1.3 Facial components, n - gross features considered in virtually all comparisons.

3. Significance and Use

3.1 Morphological analysis used for facial comparison should utilize consistent terminology and methodology. This guide provides a standard set of facial components, characteristics, and descriptors to be used as a framework in conjunction with a systematic method of analysis for facial image comparison.

3.2 The order of the facial components in this set is presented from the top of the face to the bottom, not in order of importance or priority.

3.3 Within this guide, the term “face” generally refers to the face, head, and neck inclusively unless specified otherwise.

3.4 There are several instances in this guide in which the term “distance” or “approximate distance” is used. When this term is used in this guide, it does not mean to imply that the precise value of this dimension shall be determined, but rather the relative size of this dimension compared to the overall width or height of the face, if not otherwise specified. In this guide, it is recommended that photoanthropometry not be used at all because of its limitations.

4. Facial Feature List

4.1 The following feature list contains nineteen (19) facial components, each of which is further divided into two levels of detail.

4.2 The facial components are gross features to be considered in virtually all comparisons. Tables 1 through 19 (in section 4.3) further expands each facial component into a set of component characteristics and their associated characteristic descriptors.

NOTE 1 - In the figures, dotted lines indicate the position, orientation, and/or location of the feature.

4.3 Facial Components—The human facial components are multifaceted and when imaging conditions allow, it may be possible to subdivide these components further. Any standard procedure using facial comparison analysis should consider all of the following facial components: Skin, Face/Head Outline, Face/Head Composition, Hair, Forehead, Eyebrows, Eyes, Cheeks, Nose, Ears, Mouth, Chin/Jawline, Neck, Facial Hair, Facial Lines, Scars, Facial Marks, and Alterations. If features are present and observable on a face that cannot fit into the categories below, those features should be considered and included as part of 4.3.19.

4.3.1 Skin—“Skin” refers to the overall appearance of the skin. See Table 1.

TABLE 1 Skin

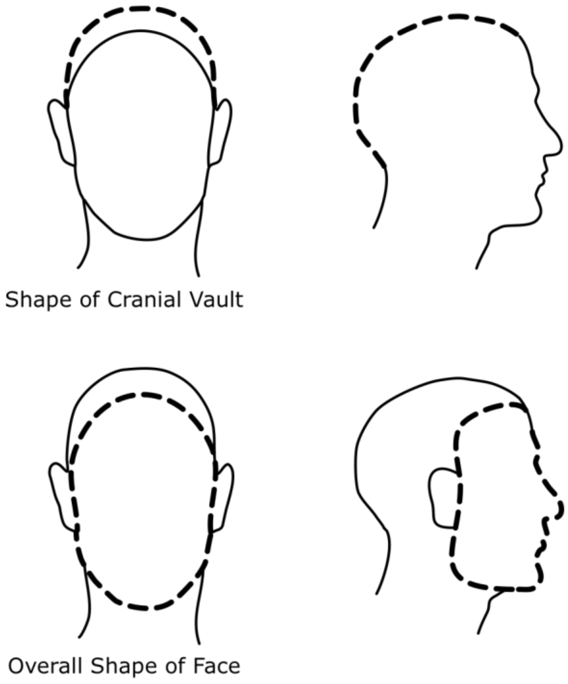
Component Characteristics	**Characteristic Descriptors**
Overall skin appearance	• Overall texture • Overall tone (for example, luminance and color)

4.3.2 Face/Head Outline - “Face/head outline” refers to the overall shape of the head (cranial vault) and face. See Table 2 and FIG 1.

TABLE 2 Face/Head Outline

Component Characteristics	**Characteristic Descriptors**
Shape of cranial vault	• Portrait contour • Profile contour
Overall shape of face	• Portrait contour • Profile contour

FIG 1 Face/Head Outline



Shape of Cranial Vault

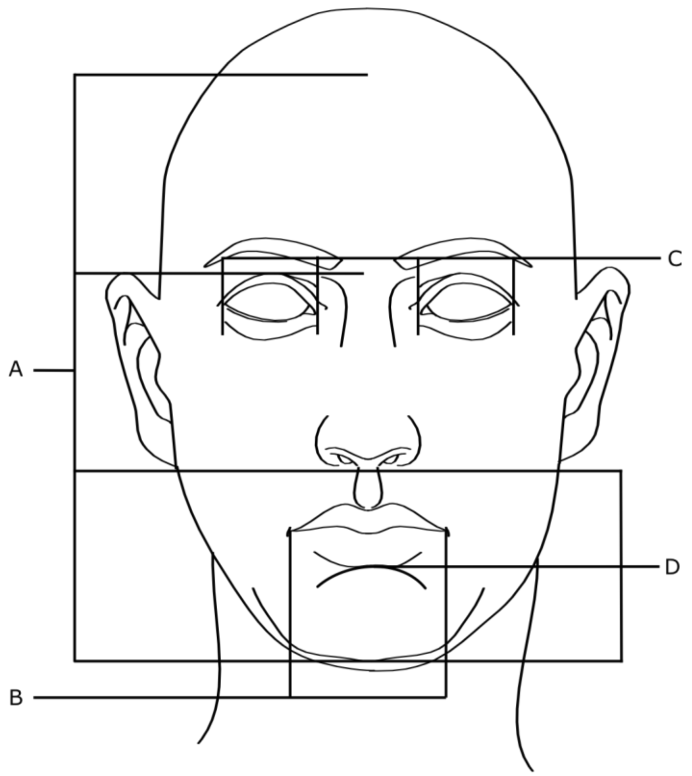
Overall Shape of Face

4.3.3 Face*/Head Composition*—"Face/head composition" refers to the overall configuration of the facial components, to include their alignment and relative sized, internal to a single face. See Table 3 and FIGS 2 and 3.

TABLE 3 Face/Head Composition

Component Characteristics	**Characteristic Descriptors**
Proportions/position of features on face	• Approximate width of nose relative to eye distances (for example, interpupillary distance, individual eye width, or overall distance between outer corners) • Approximate width of mouth relative to eye distances • Approximate width of nose relative to mouth • Approximate distance from nose to upper lip relative to face length • Approximate distance from chin to lower lip relative to face length • Ear position relative to eyes, nose, and mouth • Eye position relative to face length

FIG 2 Some of the Traditional Canons for Ideal Facial Proportions[1]



NOTE - Not all faces will conform to the proportions presented in this figure.

A - The face can be divided into three equal parts: hairline to nasal root (bridge), nasal root to nasal base, and nasal base to chin.

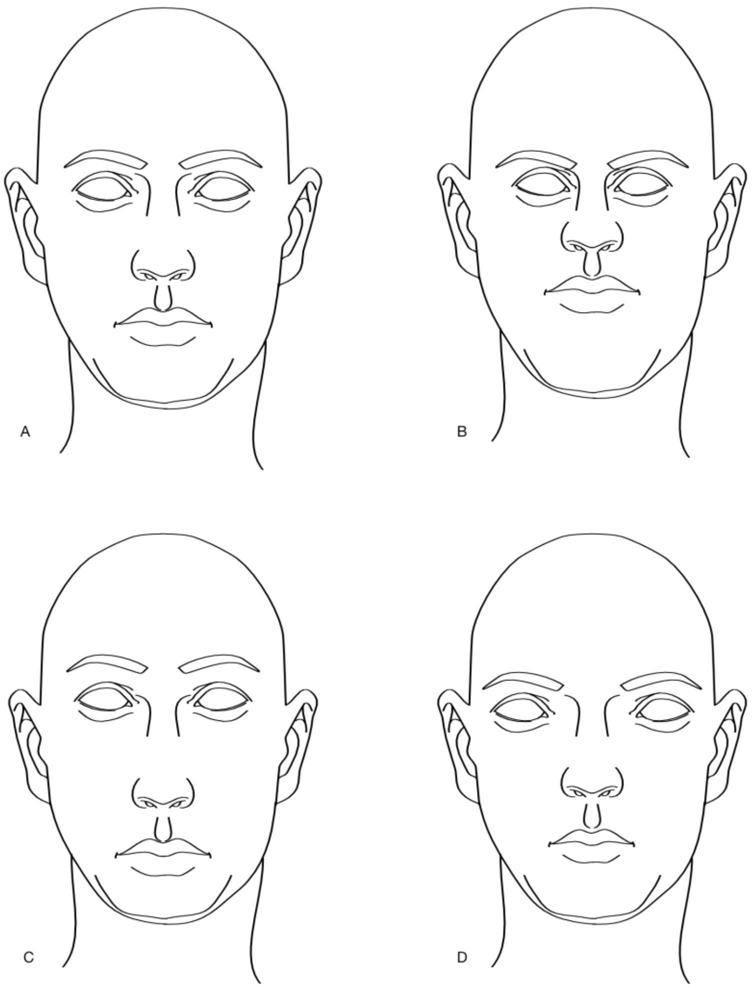
B - The width of the chin is the same as the width of the mouth.

C - The distance between the inner corners of the eyes is equal to the width of one eye.

D - The mentolabial sulcus is half the distance from the nasal base to the chin.

[1] Vegter, F. and Hage, J., "Clinical Anthropometry and Canons of the Face in Historical Perspective," *Plastic and Reconstructive Surgery,* Vol 106, No. 5, 2000, pp. 1090-1096.

FIG 3 Examples of Alterations to the Positions among Facial Components and the Effect those Positions Have on the Overall Face/Head Composition



NOTE

A - This face shows the proportions as they are presented in the previous illustration.

B - The eyes and eyebrows have been moved toward the midline (medially) and the tip of the nose, the lips, and philtrum have been raised toward the nose.

C - The eyes and eyebrows have been raised, and the tip of the nose, the lips, and philtrum have been moved down.

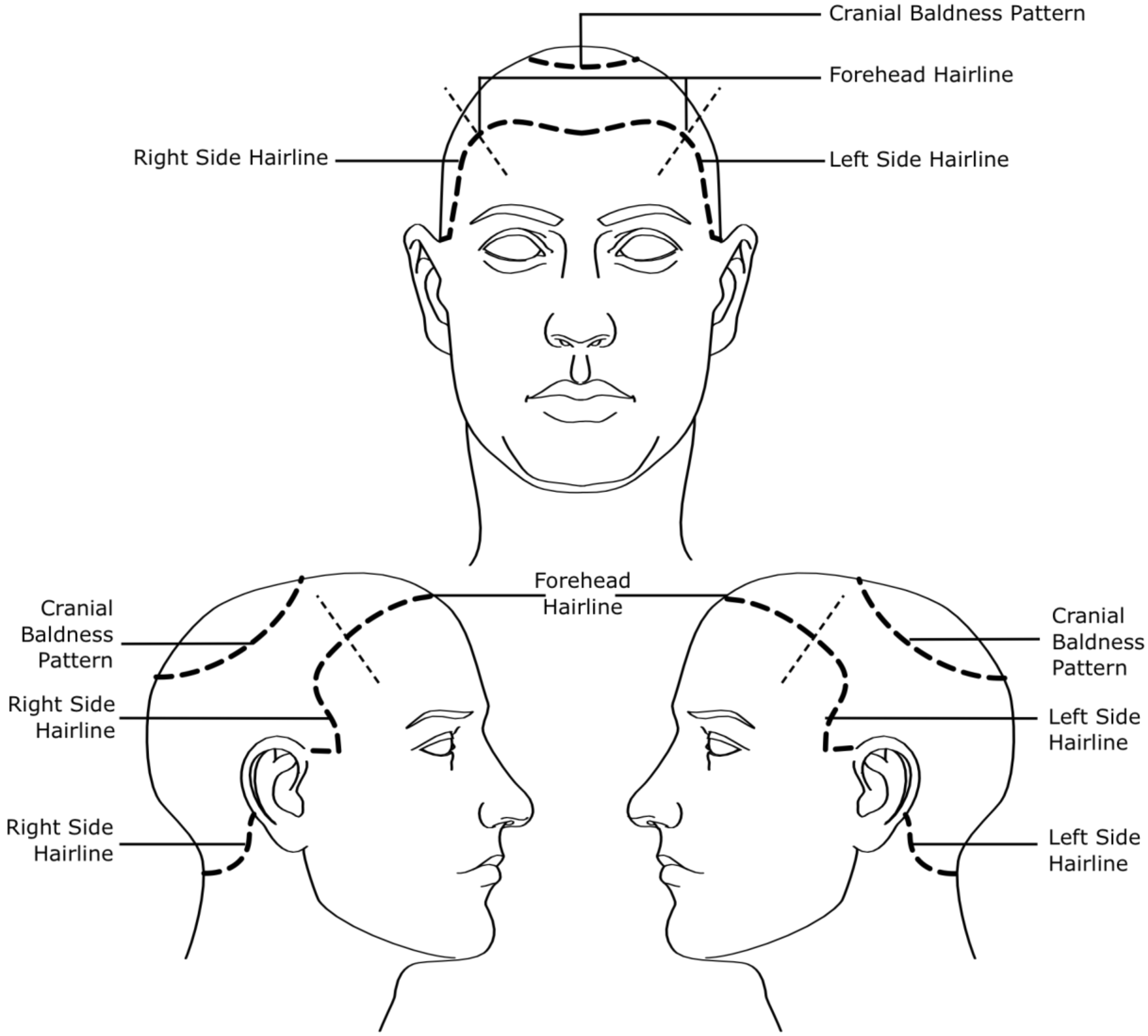
D - The eyes and eyebrows have been moved away from the midline and the lips have been made smaller. The overall face shape has not been modified in any of the figures.

4.3.4 *Hair* - Hair” refers to the shape and distribution of head hair and does not include other facial hair (eyebrows, lashes, facial hair). *Hair* includes the appearance of the hair itself and the sections of hairline and baldness patterns. Hairline refers to the contour of the edge of the hair along the top and sides of the forehead to the top of the ears. Cranial baldness pattern refers to apparent baldness affecting the hairline as well as gaps on the crown and sides of the head. See Table 4 and FIG 4.

TABLE 4 Hair

Component Characteristics	**Characteristic Descriptors**
Hair	• Shape/spatial distribution (including overall hair length) • Texture • Symmetry • Density and distribution of density (including gaps) • Tonality and variation in color/tonality
Forehead hairline	• Detailed shape (for example, symmetry, “widow’s peak,” “part line,” “cowlick”)
Hairline right side Hairline left side	• Detailed shape
Cranial baldness pattern	• Detailed shape and distribution

FIG 4 Hairline/Baldness Pattern

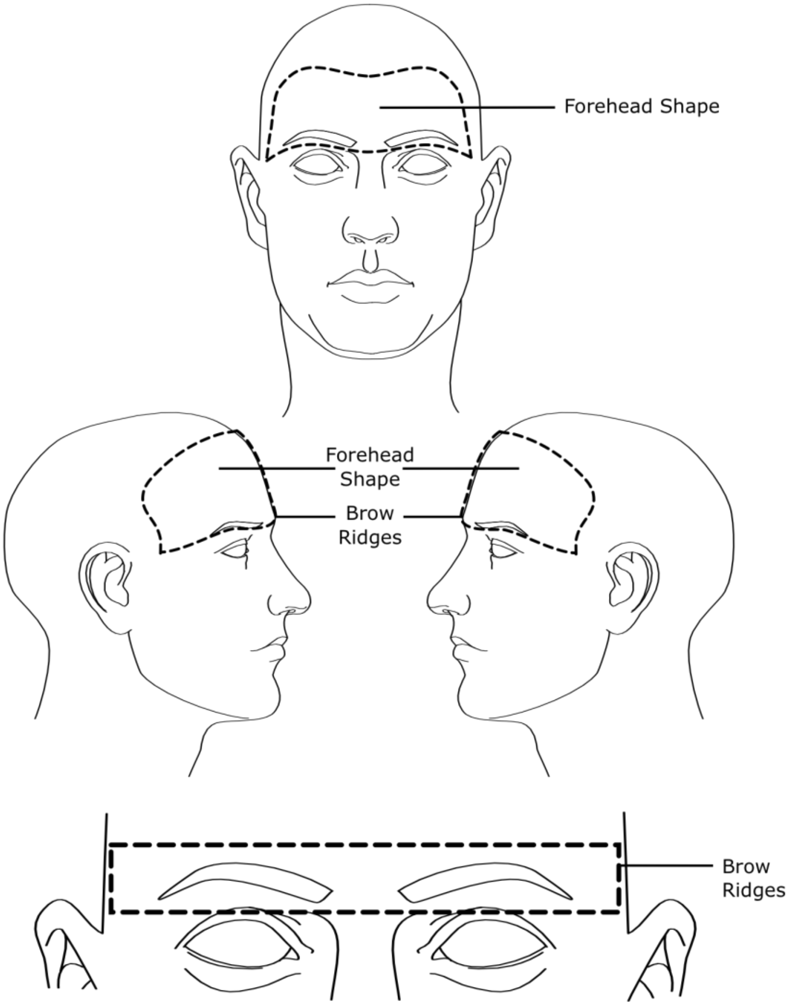


4.3.5 *Forehead* - “Forehead” refers to the part of the face above the eyes, including the brow ridges. See Table 5 and FIG 5.

TABLE 5 Forehead

Component Characteristics	**Characteristic Descriptors**
Forehead shape	• Relative height • Relative width • Slope/contour (visible in profile)
Brow ridges	• Prominence • Continuity

FIG 5 Forehead

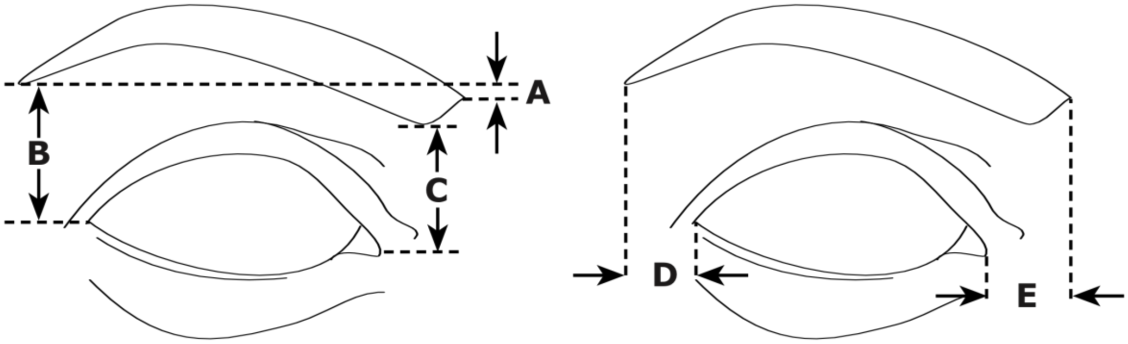


4.3.6 Eyebrows—“Eyebrows” refers to the strips of hair above the eyes. See Table 6 and FIG 6.

TABLE 6 Eyebrows

Component Characteristics	**Characteristic Descriptors**
Right eyebrow Left eyebrow	• Shape (may include detailed observations) • Size (width and length of eyebrow relative to eye size) • Lateral eyebrow vertical end position relative to medial eyebrow vertical position (tilt of eyebrow) (“A” in FIG 6) • Vertical end position of lateral eyebrow relative to the lateral canthus (“B” in FIG 6) • Vertical end position of medial eyebrow relative to the medial canthus (“C” in FIG 6) • Horizontal end position of lateral eyebrow relative to lateral canthus (“D” in FIG 6) • Horizontal end position of medial eyebrow relative to medial canthus (“E” in FIG 6) • Conjoined left-right eyebrows (“unibrow”) • Density of hair within eyebrow and distribution of density • Hair details (for example, texture, length, thickness, shape, and color) • Noticeably longer hairs
Asymmetry between right and left eyebrows	• Overall shape, size, position, hair details, and so forth (see individual eyebrow descriptors)

FIG 6 Position of the Eyebrow Relative to the Position of the Eye Opening



NOTE -

A—Lateral eyebrow vertical end position relative to medial eyebrow vertical position.

B—Vertical end position of lateral eyebrow relative to the lateral canthus.

C—Vertical end position of medial eyebrow relative to the medial canthus.

D—Horizontal end position of lateral eyebrow relative to the lateral canthus.

E—Horizontal end position of medial eyebrow relative to the medial canthus.

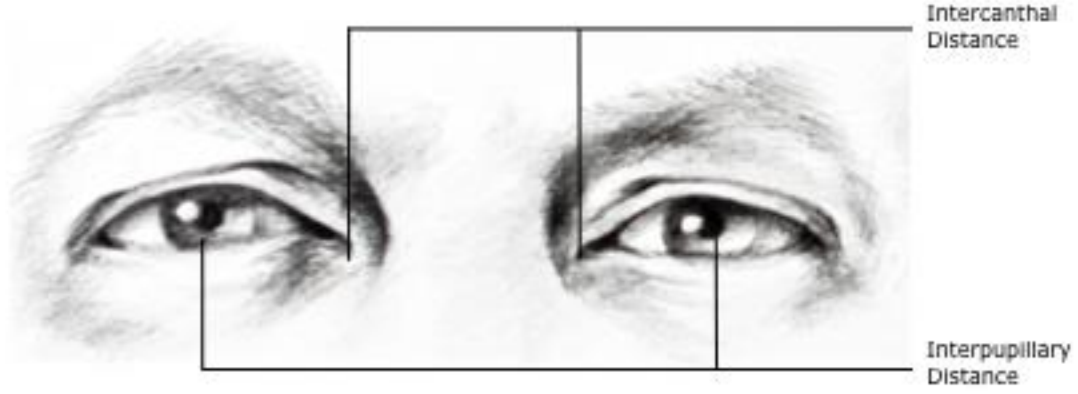
4.3.7 *Eyes*—"Eyes" refers to the orbital region below the eyebrows and above the cheeks. See Table 7 and FIGS 7-9.

TABLE 7 Eyes

Component Characteristics	**Characteristic Descriptors**
Intercanthal distance	• Distance between inner corners of the right and left eyes
Interpupillary distance	• Distance between the center of the right and left pupils
Right eye fissure opening Left eye fissure opening (outline)	• Shape • Angle [angle from inner corner and outer corner (when eyes are horizontal)]
Right upper eyelid Left upper eyelid (including lashes)	• Prominence (for example, visibility, folds, including epicanthic fold) • Protrusion • Visibility of the crease above the upper eyelid (superior palpebral furrow) • Position in relation to iris and/or pupil • Lash characteristics (for example, length, density, flow, irregular)
Right lower eyelid Left lower eyelid (including lashes)	• Prominence (for example, visibility, folds) • Protrusion • Visibility of the crease below the lower eyelid (inferior palpebral furrow) • Visibility of infraorbital furrow (a place where a line or wrinkle may appear parallel to and below the lower eyelid running from near the inner canthus and following cheek bone laterally) • Position in relation to iris and/or pupil • Lash characteristics (for example, length, density, flow, irregular)
Right eyeball prominence Left eyeball prominence	• Degree of protrusion
Right eye sclera Left eye sclera	• Visibility of blood vessels and defects • Color
Right iris Left iris	• Color • Visibility • Diameter relative to eye opening • Position relative to eye opening (in front view) • Irregularity in pupil

Component Characteristics	**Characteristic Descriptors**
Right eye medial canthus Left eye medial canthus	• Caruncle (fleshy prominence at inner eye corner) • Shape and angle of inner corner of the eye
Right eye lateral canthus Left eye lateral canthus	• Shape and angle of outer corner of the eye
Asymmetry between right and left eyes	• Shape, angle • Off-set (for example, one eye higher than the other) • Eyelids (for example, one drooping, one retracted) and eyelashes • Color • Iris and pupil position (for example, cross-eyed) • Overall shape, size, position, and so forth (see individual eye descriptors)

FIG 7 Eyes


Intercanthal Distance
Interpupillary Distance

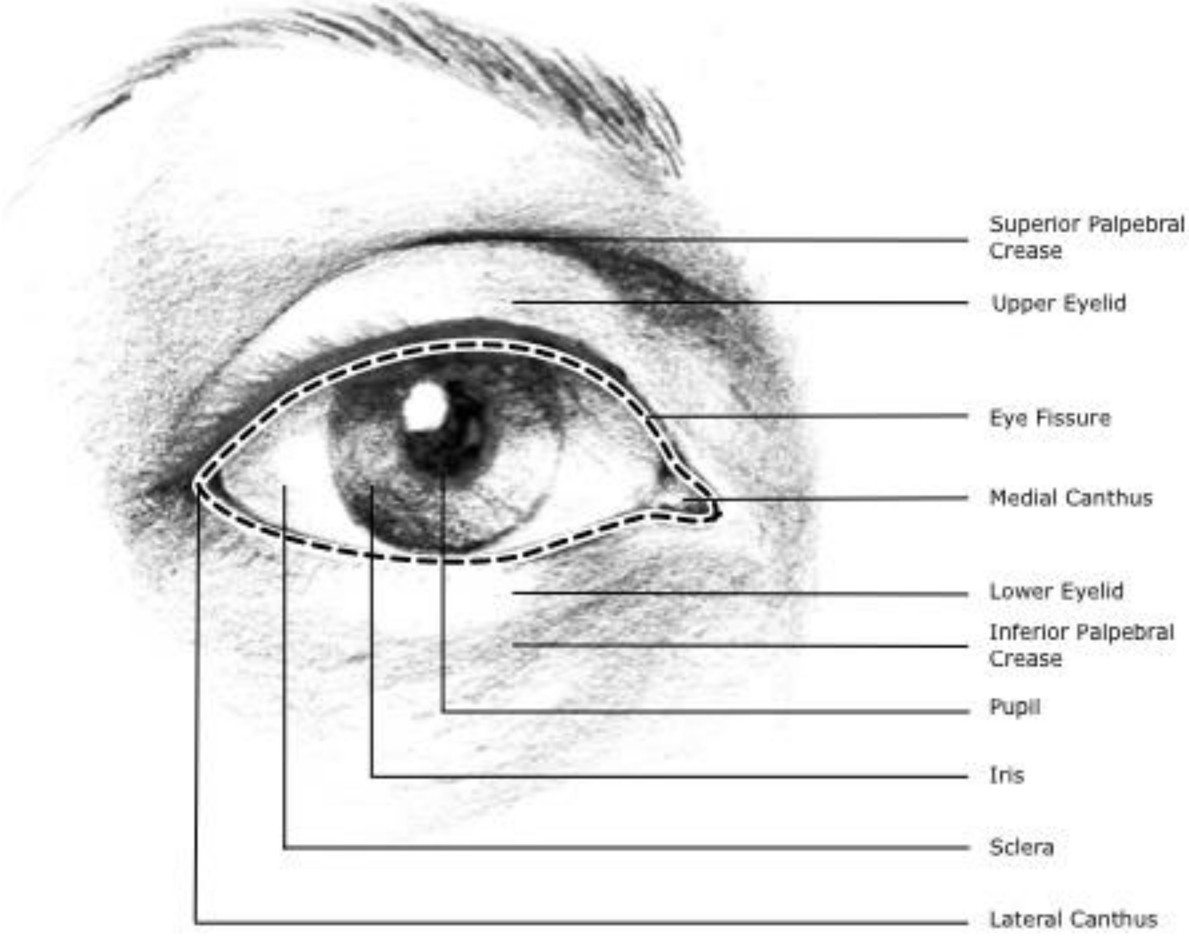
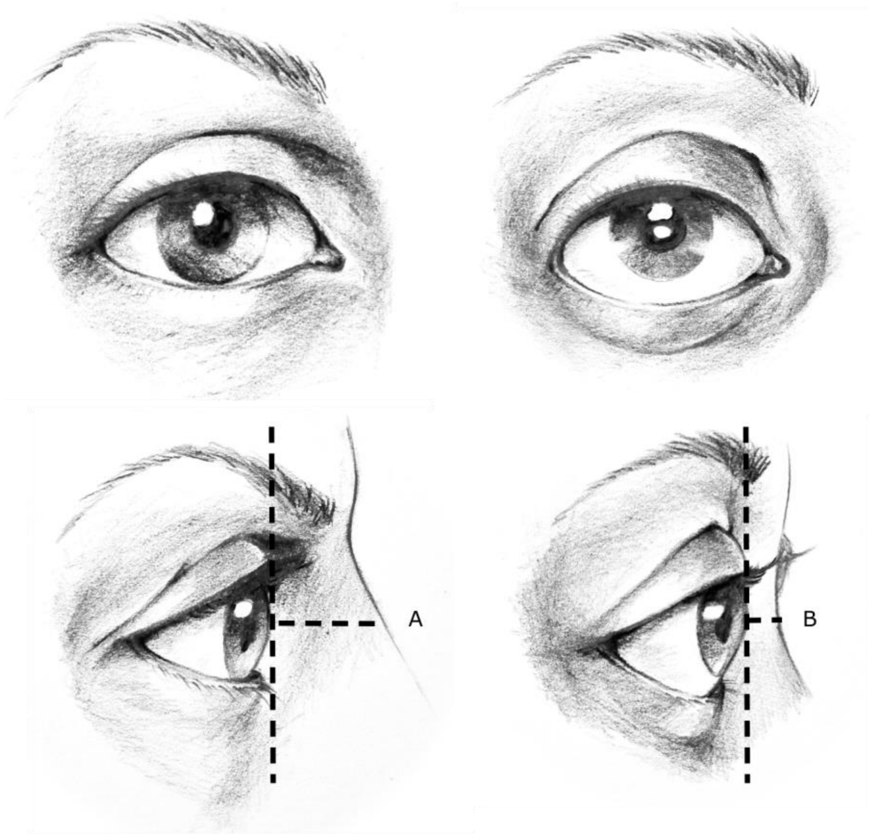

Superior Palpebral Crease
Upper Eyelid
Eye Fissure
Medial Canthus
Lower Eyelid
Inferior Palpebral Crease
Pupil
Iris
Sclera
Lateral Canthus

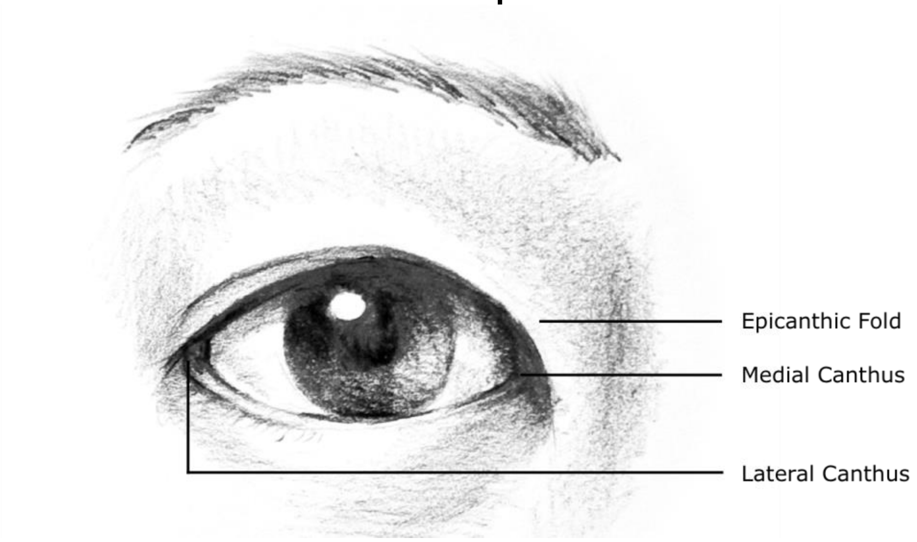
FIG 8 Anterior (Forward) Projection of the Eyes

Eyeball Prominence



NOTE - **A** shows an eye with minimal prominence (projection forward from the socket), whereas **B** shows an eye with significant prominence.

FIG 9 Epicanthic Fold



4.3.8 *Cheeks*—"Cheeks" refers to the regions surrounded by the eyes, ears, nose, mouth, chin, and jawline. See Table 8.

TABLE 8 Cheeks

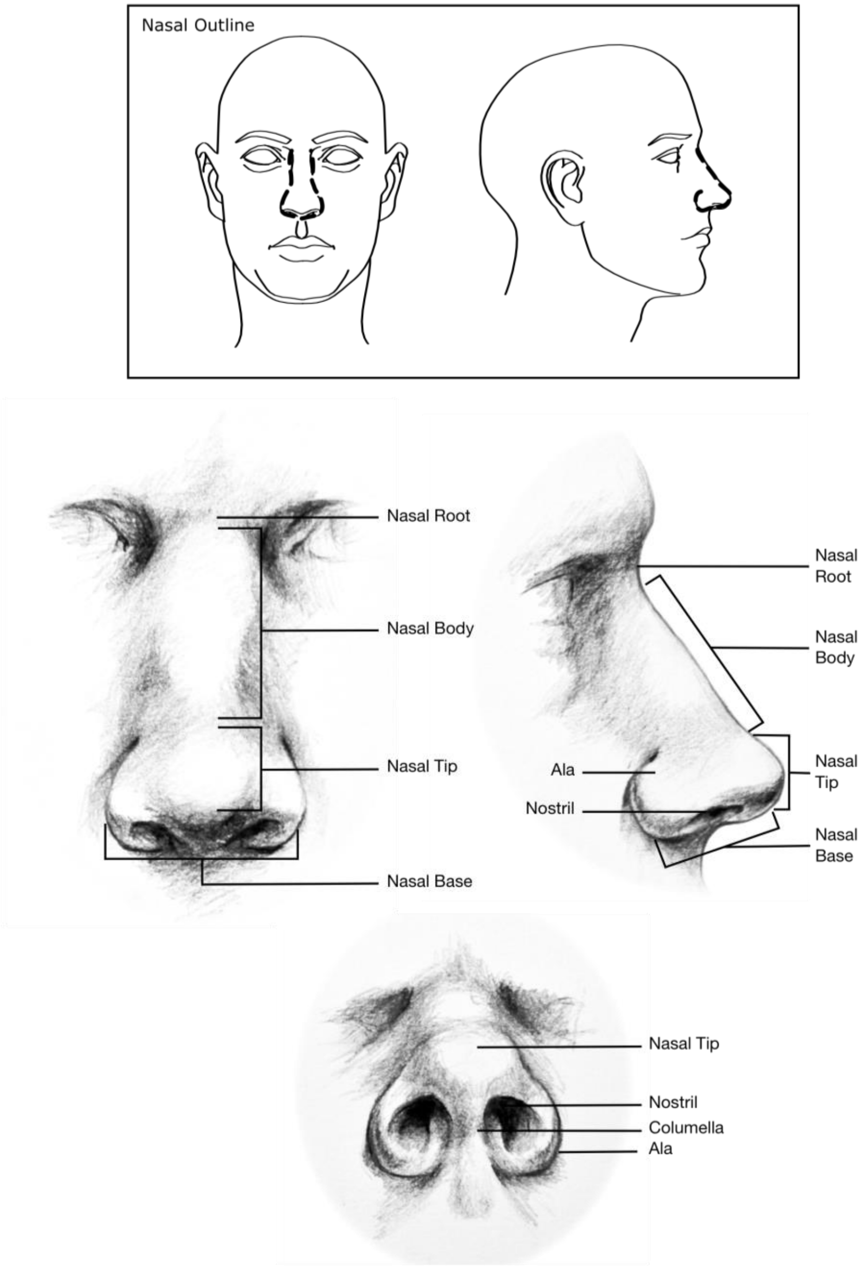
Component Characteristics	**Characteristic Descriptors**
Right cheekbone Left cheekbone	• Prominence
Right cheek shape Left cheek shape (soft tissue)	• Presence of dimple

4.3.9 *Nose*—"Nose" refers to the entire nasal region. See Table 9 and FIG 10.

TABLE 9 Nose

Component Characteristics	**Characteristic Descriptors**
Nasal outline (profile and front view)	• Overall shape • Length or width or both • Prominence • Symmetry
Nasal root (bridge)	• Front view: *w*idth, length, shape, depth • Profile view: length, depth, angle
Nasal body	• Front view: *w*idth, length, shape, angle • Profile view: length, angle, contour
Nasal tip	• Shape (in front and profile view, including whether or not the tip is bifid) • Angle (for example, up, down) • Symmetry
Nasal base	• Width • Height • Deviation to the right or left
Nasal base: alae (wings of nose)	• Thickness • Symmetry • Shape
Nasal base: nostrils (nasal openings)	• Shape and size of opening • Symmetry • Hair
Nasal base: columella (soft tissue between nostrils)	• Width and length • Relative position • Symmetry

FIG 10 Nose


Nasal Outline
Nasal Root
Nasal Body
Nasal Tip
Nasal Base
Nasal Root
Nasal Body
Ala
Nostril
Nasal Tip
Nasal Base
Nasal Tip
Nostril
Columella
Ala

4.3.10 *Ears*—"Ears" refers to the external characteristics of the ears. See Table 10 and FIGS 11 and 12.

TABLE 10 Ears

Component Characteristics	**Characteristic Descriptors**
Asymmetry between left and right ears	• Size • Shape • Protrusion • Positioning (for example, one higher than the other)
Right ear protrusion Left ear protrusion	• Extent of protrusion
Overall right ear Overall left ear	• Size • Shape • Angle
Right ear helix—superior/inferior (tail) Left ear helix—superior/inferior (tail)	• Size • Shape
Right ear tubercles (auricular/Darwin's tubercle) Left ear tubercles (auricular/Darwin's tubercle)	• Size • Shape • Quantity
Right ear antihelix Left ear antihelix	• Size • Shape
Right ear crura of antihelix (superior crux, inferior crux) Left ear crura of antihelix (superior crux, inferior crux)	• Size • Shape
Right ear triangular fossa Left ear triangular fossa	• Size • Shape
Right ear crus of helix Left Ear crus of helix	• Size • Shape
Right ear scaphoid fossa Left ear scaphoid fossa	• Size • Shape

Component Characteristics	**Characteristic Descriptors**
Right ear concha (superior, inferior) Left ear concha (superior, inferior)	• Size • Shape
Right ear tragus Left ear tragus	• Size • Shape • Protrusion
Right ear antitragus Left ear antitragus	• Size • Shape • Protrusion
Right ear intertragic/intertragal notch Left ear intertragic/intertragal notch	• Size • Shape
Right ear anterior knob Left ear anterior knob	• Size • Shape
Right ear anterior notch Left ear anterior notch	• Size • Shape
Right ear posterior auricular furrow Left ear posterior auricular furrow	• Size • Shape
Right ear lobule (lobe) Left ear lobule (lobe)	• Size • Shape • Attached or detached
Ear abnormalities	• For example, cleft lobe, “cauliflower ear”

FIG 11 Ear Position

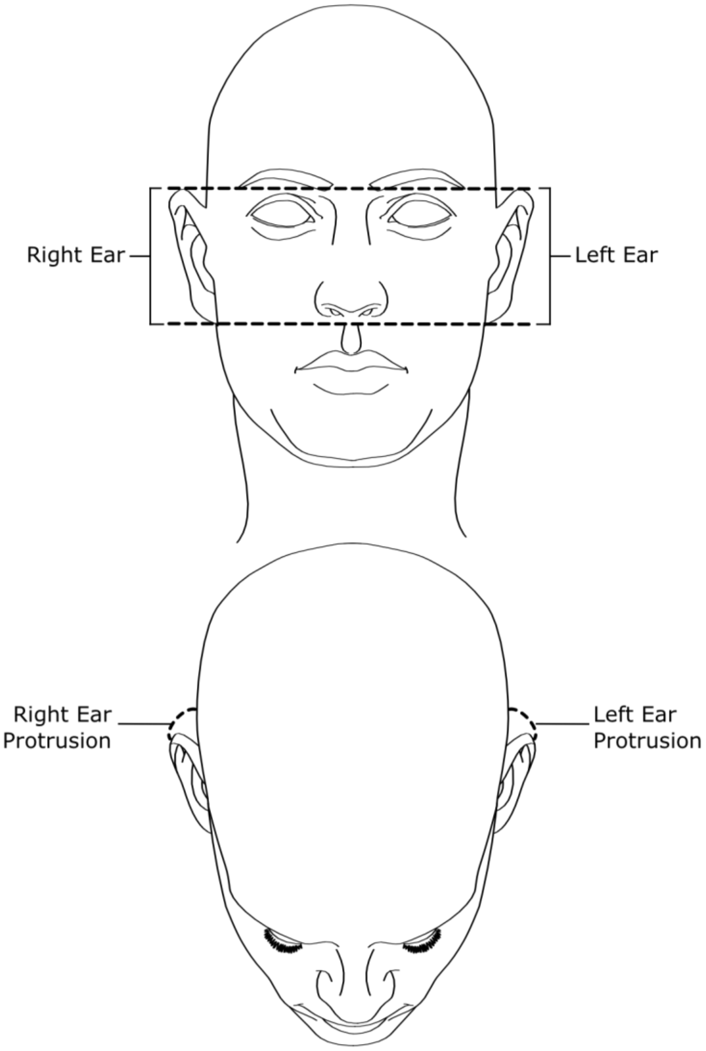
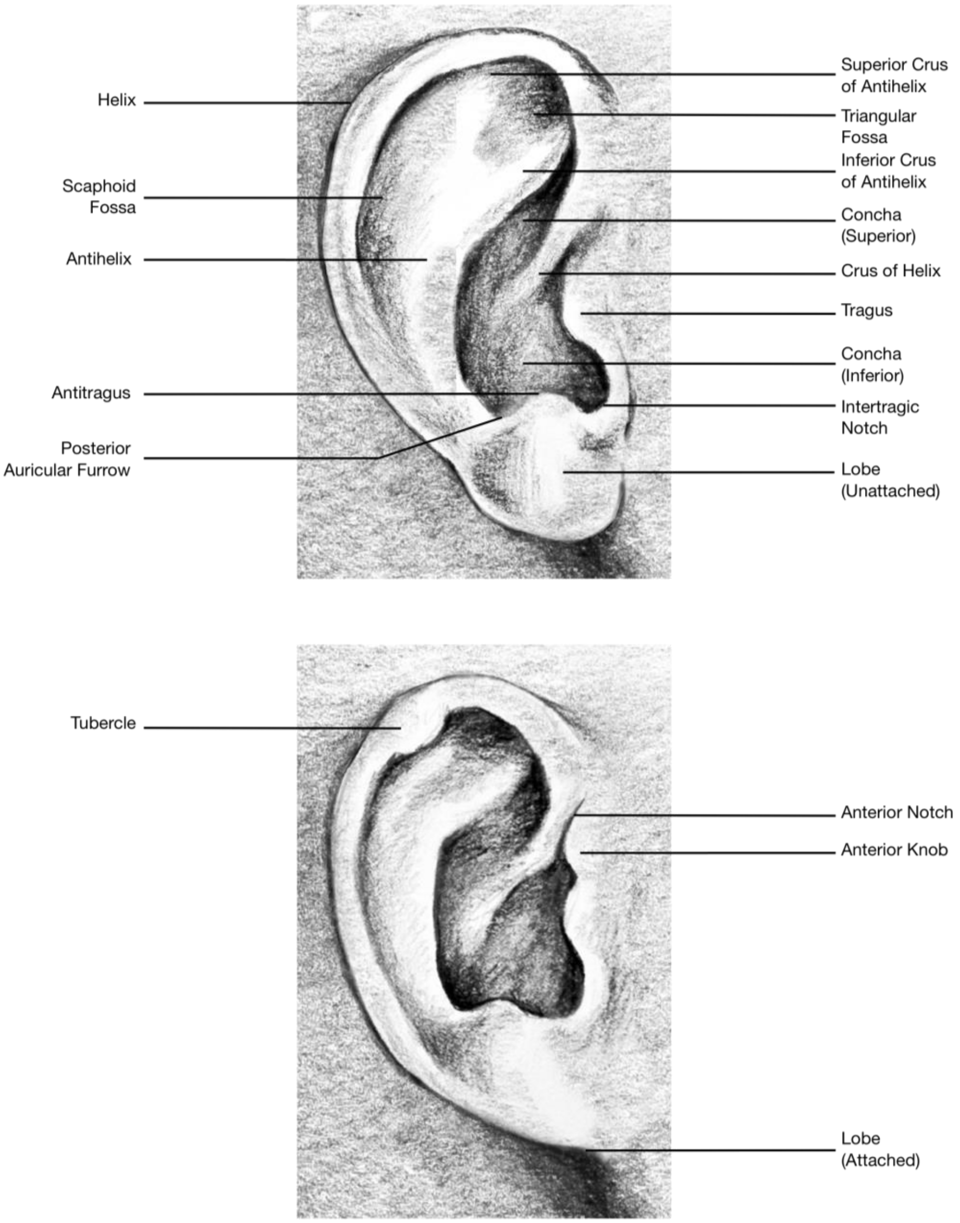


FIG 12 Ear


Helix
Scaphoid Fossa
Antihelix
Antitragus
Posterior Auricular Furrow
Superior Crus of Antihelix
Triangular Fossa
Inferior Crus of Antihelix
Concha (Superior)
Crus of Helix
Tragus
Concha (Inferior)
Intertragic Notch
Lobe (Unattached)
Tubercle
Anterior Notch
Anterior Knob
Lobe (Attached)

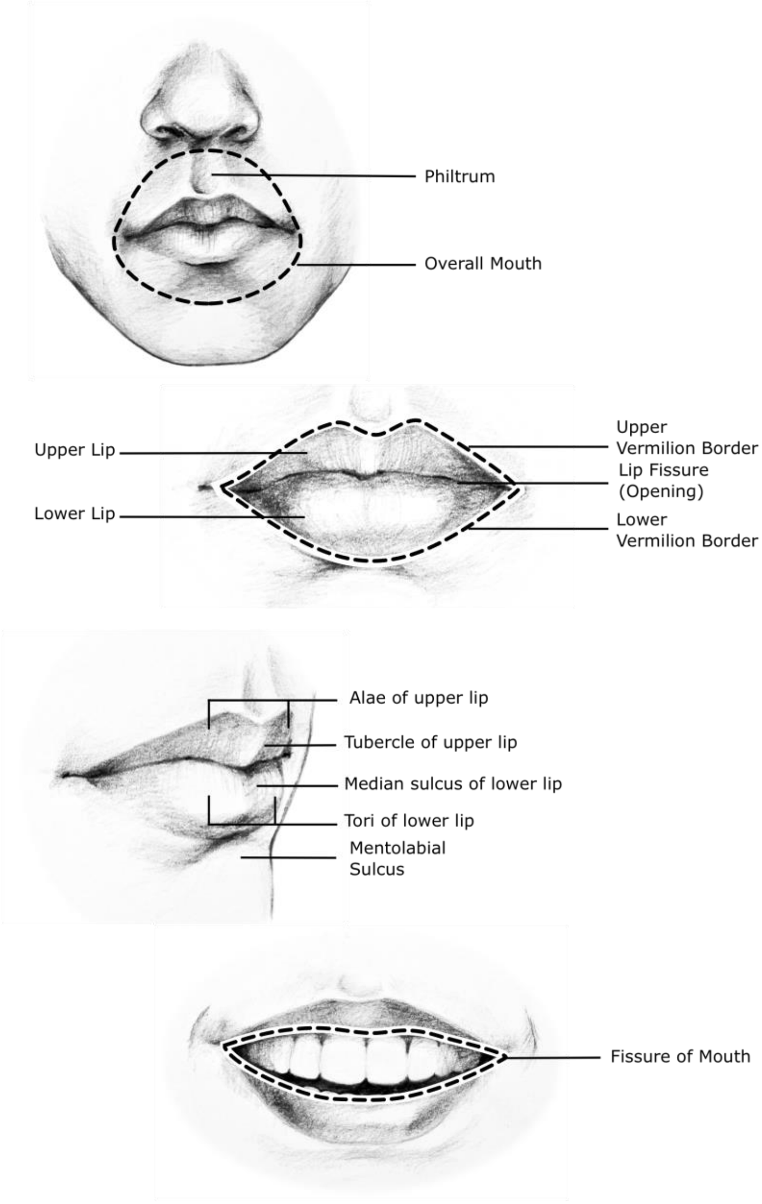
4.3.11 *Mouth*—"Mouth" refers to the entire oral region including the teeth and encompasses the philtrum. See Table 11 and FIG 13.

TABLE 11 Mouth

Component Characteristics	**Characteristic Descriptors**
Philtrum	• Prominence • Width of ridges • Width of furrow • Symmetry
Overall mouth	• Shape • Symmetry
Upper lip	• Shape • Fullness • Protrusion • Symmetry • Upper vermilion border shape (for example, "Cupid's bow") and definition • Detail (for example, tubercle, lip creases, alae)
Lower lip	• Shape • Fullness • Protrusion • Symmetry • Lower vermilion border shape and definition • Detail (for example, median sulcus, tori, lip creases)
Lip fissure (opening between lips)	• Shape • Symmetry • Degree of contact/occlusion along length of opening • Corners/angles of mouth (labial commissure)
Mouth asymmetry	• Difference between left and right sides
Overall dental occlusion (contact between upper and lower teeth)	• Symmetry • Degree of contact/occlusion
Gnathism (apparent convexity or concavity of the mouth complex, related to the relative projection of the upper and/or lower teeth)	• Expression (for example, upper gums/teeth protrude, lower gums/teeth protrude) • Degree •

Component Characteristics	Characteristic Descriptors
Characteristic detail of teeth	• Shape • Size • Alignment/position (for example, gaps, crooked, missing) • Condition (for example, wear, damage, disease, color)
Mouth abnormalities	• For example, cleft lip (congenital deformity caused by abnormal facial development during gestation)

FIG 13 Mouth

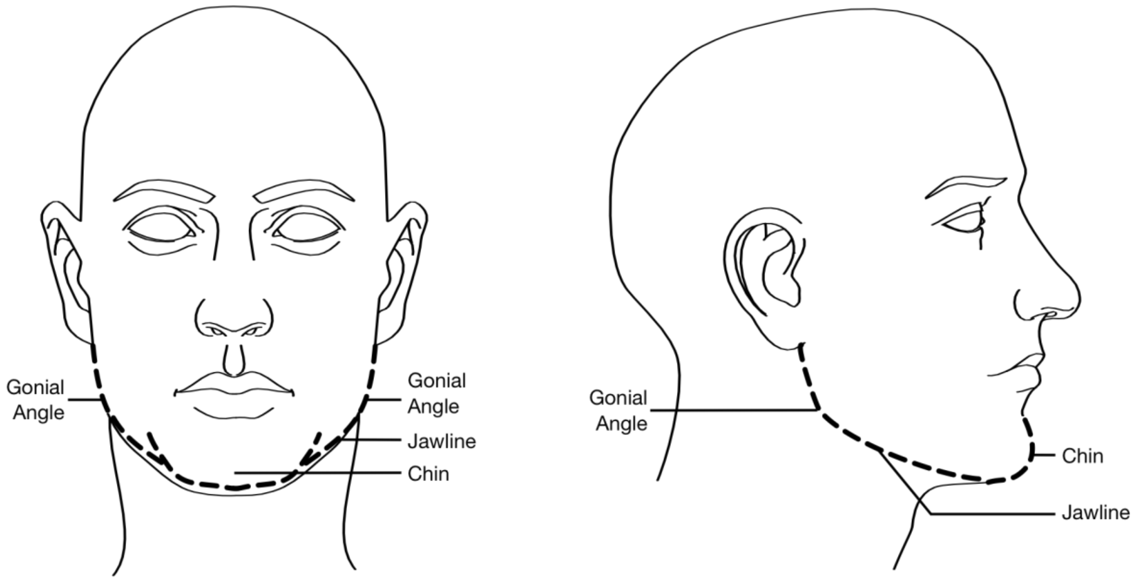

Philtrum
Overall Mouth
Upper Lip
Lower Lip
Upper Vermilion Border
Lip Fissure (Opening)
Lower Vermilion Border
Alae of upper lip
Tubercle of upper lip
Median sulcus of lower lip
Tori of lower lip
Mentolabial Sulcus
Fissure of Mouth

4.3.12 *Chin/Jawline*—"Chin/jawline" refers to the area of the face defined by the lower border of the mandible (namely, "jaw bone"). The chin is the area on the lower jaw below the mouth. Jawline specifically refers to the area of the face defined by the lower border of the mandible between the chin and the gonial angle or the point at which the lower border of the mandible abruptly changes direction from a primarily horizontal line to a primarily vertical line. See Table 12 and FIG 14.

TABLE 12 Chin/Jawline

Component Characteristics	**Characteristic Descriptors**
Chin (profile and frontal view)	• Overall shape • Length or width or both relative to rest of face • Prominence • Symmetry • Details (for example, cleft, dimple, mental groove; refer to 4.18 Facial Lines)
Jawline (from chin to gonial angle)	• Shape • Definition (for example, jowls)
Gonial angle (angle of the jaw)	• Shape • Definition

FIG 14 Chin/Jawline

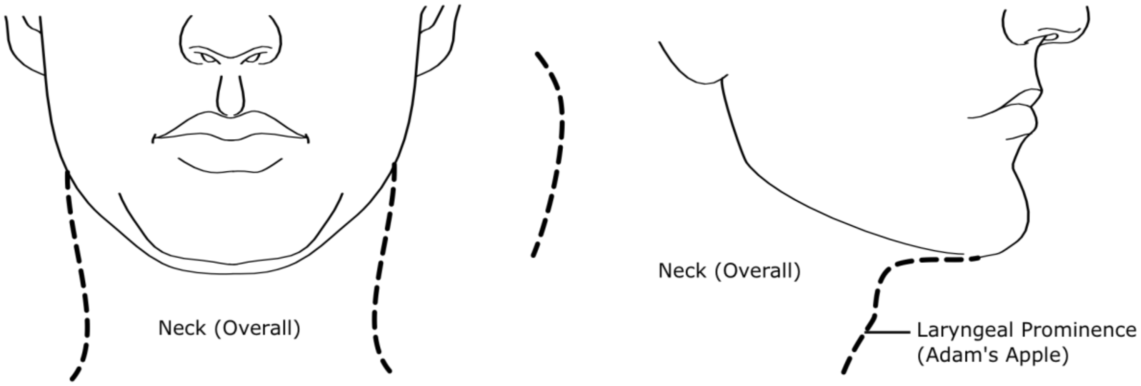


4.3.13 Neck—“Neck” refers to the transitional zone between the head and the trunk and limbs of the body. See Table 13 and FIG 15.

TABLE 13 Neck

Component Characteristics	Characteristic Descriptors
Neck (overall)	• Width • Height • Details (for example, musculature, veins, wrinkles, folds, “wattle,” “double chin”)
Laryngeal prominence (Adam's apple)	• Shape • Size • Prominence • Location on neck

FIG 15 Neck



4.3.14 *Facial Hair*—“Facial hair” refers to the hair on the face typically covering the cheeks, chin/jaw, upper and lower lip, and neck of the face. See Table 14.

TABLE 14 Facial Hair

Component Characteristics	Characteristic Descriptors
Facial hair above upper lip Facial hair below lower lip	• Shape/spatial distribution (including overall hair length) • Texture • Symmetry • Density and distribution of density including gaps • Variation in color/tonality • Orientation (slanted, straight) • Outline/edge definition (for example, sharp, irregular) • Continuity with facial hair on side(s) or below/above mouth • Noticeably longer hairs
Facial hair on right side Facial hair on left side	• Shape/spatial distribution (including overall hair length) • Texture • Symmetry • Density and distribution of density including gaps • Variation in color/tonality • Orientation (slanted, straight) • Outline/edge definition (for example, sharp, irregular) • Continuity with facial hair above or below mouth • Noticeably longer hairs
Facial hair on neck, below chin/jawline	• Shape/spatial distribution (including overall hair length) • Texture • Symmetry • Density and distribution of density including gaps • Variation in color/tonality • Orientation (slanted, straight) • Outline/edge definition (for example, sharp, irregular) • Continuity with facial hair on side(s) or below mouth Noticeably longer hairs

4.3.15 *Facial Lines*—“Facial Lines” refers to wrinkles, folds, or creases. Creases or folds are determined by craniofacial structure. Other lines, such as wrinkles, are age-related and are caused by muscle action, loss of elasticity of the skin, and/or loss of subcutaneous fat/teeth at sunken areas. The following list represents the most common facial lines and is not an exhaustive list. Special attention should be paid to any lines that do not correspond to those listed below. See Table 15 and FIG 16.

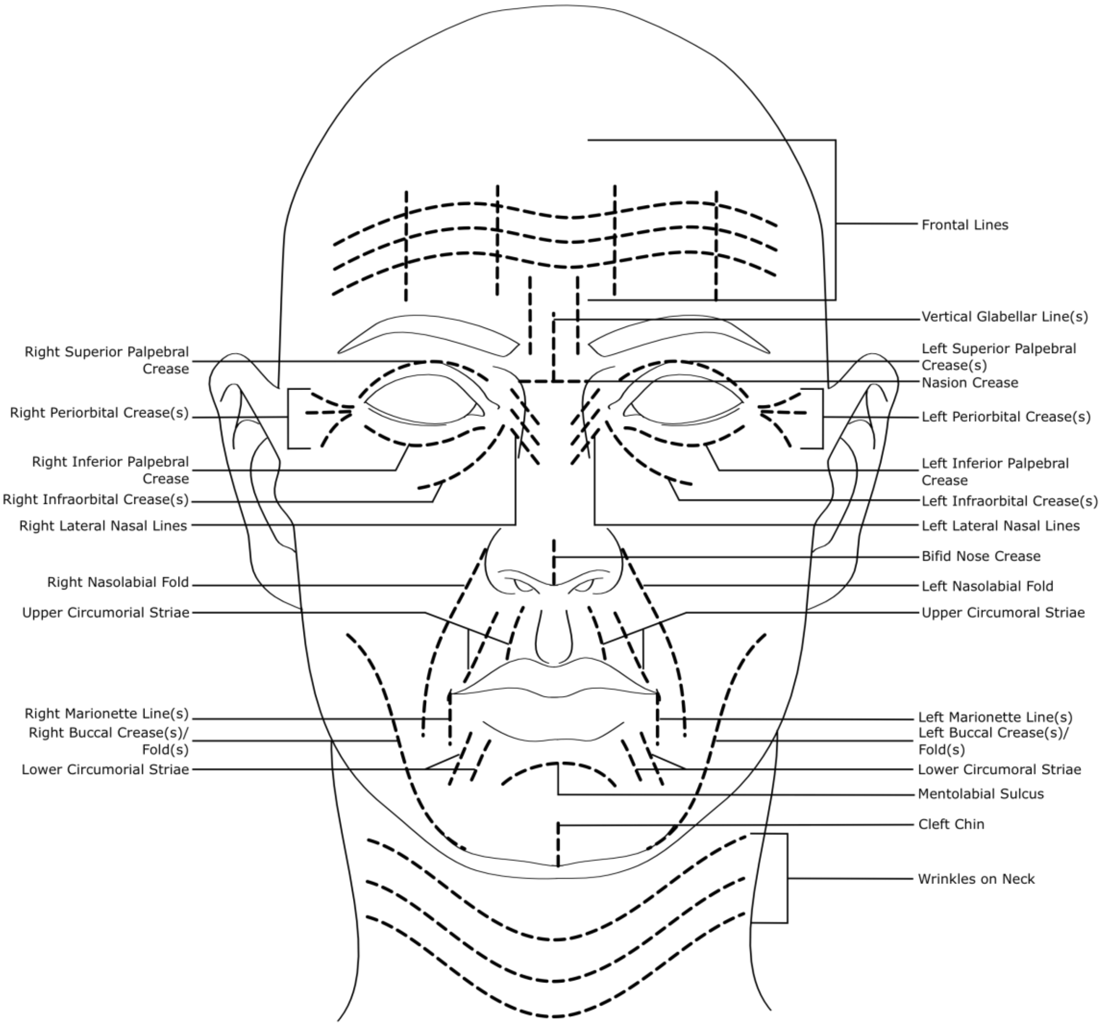
TABLE 15 Facial Lines

Component Characteristics	**Characteristic Descriptors**
Frontal lines (forehead wrinkles)	• Distribution • Orientation (vertical or horizontal) • Quantity • Pattern (including relation to one another) • Depth/prominence
Vertical glabellar line(s)	• Length • Pattern (including relation to one another) • Depth/prominence
Nasion crease	• Distribution • Quantity • Pattern (including relation to one another) • Depth/prominence
Right lateral nasal lines Left lateral nasal lines	• Distribution • Orientation • Quantity • Pattern (including relation to one another) • Depth/prominence
Bifid nose crease	• Depth/prominence • Length
Periorbital lines adjacent to right eye (Crow's Feet/wrinkles) Periorbital lines adjacent to left eye (crow's feet/wrinkles)	• Distribution • Quantity • Pattern (including relation to one another) • Depth/prominence

Component Characteristics	Characteristic Descriptors
Right superior palpebral crease Left superior palpebral crease (crease between the upper eyelid and the top of the bony orbit)	• Visibility • Position • Depth/prominence • Shape
Right inferior palpebral crease Left inferior palpebral crease (crease between the lower eyelid and the bottom of the bony orbit)	• Visibility • Position • Depth/prominence • Shape
Right infraorbital creases Left infraorbital creases (creases below the eyes)	• Distribution • Quantity • Pattern (including relation to one another) • Depth/prominence
Upper circumoral striae (lines above upper lip) Lower circumoral striae (lines below lower lip)	• Distribution • Quantity • Pattern (including relation to one another) • Depth/prominence
Mentolabial sulcus (horizontal crease or fold between lower lip and chin)	• Shape • Length • Depth/prominence
Right nasolabial crease/folds Left nasolabial crease/folds (creases or folds extending from nose to corners of mouth)	• Distribution • Quantity • Pattern (including relation to one another) • Depth/prominence
Right marionette lines Left marionette lines	• Pattern • Depth/prominence
Cleft chin	• Depth/prominence • Size
Right buccal creases/folds Left buccal creases/folds (cheek to chin)	• Distribution • Quantity • Pattern (including relation to one another) • Depth/prominence

Component Characteristics	Characteristic Descriptors
Wrinkles on neck	• Distribution • Quantity • Pattern (including relation to one another) • Depth/prominence
Other creases	• Distribution • Quantity • Pattern (including relation to one another) • Depth/prominence

FIG 16 Facial Lines


Frontal Lines
Vertical Glabellar Line(s)
Right Superior Palpebral Crease
Left Superior Palpebral Crease(s)
Nasion Crease
Right Periorbital Crease(s)
Left Periorbital Crease(s)
Right Inferior Palpebral Crease
Left Inferior Palpebral Crease
Right Infraorbital Crease(s)
Left Infraorbital Crease(s)
Right Lateral Nasal Lines
Left Lateral Nasal Lines
Bifid Nose Crease
Right Nasolabial Fold
Left Nasolabial Fold
Upper Circumorial Striae
Upper Circumoral Striae
Right Marionette Line(s)
Left Marionette Line(s)
Right Buccal Crease(s)/ Fold(s)
Left Buccal Crease(s)/ Fold(s)
Lower Circumorial Striae
Lower Circumoral Striae
Mentolabial Sulcus
Cleft Chin
Wrinkles on Neck

4.3.16 Scars—“Scars” refers to dysmorphic or discolored areas or both of skin where permanent damage has healed (that is, not recent damage). These areas may occur at any place on the face since they are typically caused by random trauma or intentional scarification (for example, branding). See Table 16.

TABLE 16 Scars

Component Characteristics	Characteristic Descriptors
Scars	• Location • Shape • Orientation • Size • Color/tonality • Depth/prominence

4.3.17 *Facial Marks*—“Facial Marks” refers to portions of the skin that contain a different level of pigment than the rest of the surrounding skin (for example, freckles, moles, acne, rosacea, birth marks, bruises, abrasions, vitiligo, and dark/light patches). These areas may occur in any location of the face since they are typically random in nature. Some facial marks are transient features that require contemporaneous images for comparison (for example, acne, bruises, and abrasions). See Table 17.

TABLE 17 Facial Marks

Component Characteristics	Characteristic Descriptors
Skin marks (for example, freckles, moles, acne, rosacea, birth marks, bruises, abrasions, vitiligo, and dark/light patches)	• Location/distribution (including relation to one another) • Shape • Size • Color • Prominence

4.3.18 *Alterations*—“Alterations” refers to any intentional modification to the face with the exception of scarring. See Table 18.

TABLE 18 Alterations

Component Characteristics	**Characteristic Descriptors**
Piercing	• Location • Description
Makeup	• Location • Description (for example, shape, size, and color)
Tattoo (including cosmetic)	• Location • Description (for example, content, shape, size, and color)
Other	• Location • Description

4.3.19 *Other*—The suite of components and characteristics identified in the paragraphs above should be sufficient to address the vast majority of faces encountered in facial comparison situations. However, in some instances, there may be deformities or other irregularities on a face that do not conform to this set of features. In such instances, it will be necessary to include these irregular features in the analysis. Given the unconstrained range of possibilities that this component set represents, it is simply labeled as “other.” See Table 19.

TABLE 19 Other

Detailed Feature Characteristic List	**Feature Attribute List**
Other text	• Description • Details

5. Keywords

5.1 facial comparison; facial features; morphological analysis

BIBLIOGRAPHY

Gray, H., *Gray's Anatomy, 35th Edition,* P. L. Williams and R. Warwick, Eds., Churchill Livingstone, London, 1973.

Taylor, K. T., *Forensic Art and Illustration*, CRC Press, Boca Raton, FL, 2001.

Wilkinson, C., *Forensic Facial Reconstruction*, Cambridge University Press, Cambridge, UK, 2004.

Wankmiller, J., illustrations in this document